

5

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT

In re application of: Yuusaku FUJII et al..

Serial No.: Not Yet Assigned

Filed: October 22, 1999

For: ILLEGAL ACCESS DISCRIMINATING APPARATUS AND METHOD

CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Assistant Commissioner for Patents
Washington, D.C. 20231

October 22, 1999

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

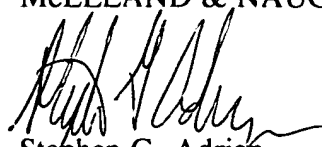
Japanese Appln. No. 10-302008, filed on October 23, 1998

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicants have complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI
McLELAND & NAUGHTON


Stephen G. Adrian
Reg. No. 32,878

Atty. Docket No.: 991176
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
Fax: (202) 887-0357
SGA/yap



jc511 U.S. PTO
09/425736
10/22/99

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following
application as filed with the Office.

Date of Application : October 23, 1998

Application Number : Patent Application No.Heisei 10-302,008

Applicant (s) : FUJITSU LIMITED

August 31, 1999

Commissoner, Takeshi Isayama
Patent Office

Certificate No.Hei 11-3061331

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JCS11 U.S. PRO
09/425736
10/22/99

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application: 1998年10月23日

出 願 番 号
Application Number: 平成10年特許願第302008号

出 願 人
Applicant(s): 富士通株式会社

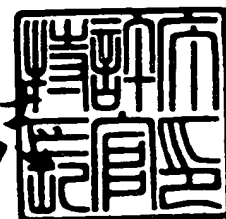
CERTIFIED COPY OF
PRIORITY DOCUMENT

Best Available Copy

1999年 8月31日

特許庁長官
Commissioner,
Patent Office

山 佐 建 彦



出証番号 出証特平11-3061331

【書類名】 特許願

【整理番号】 9803728

【提出日】 平成10年10月23日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/30
G06F 15/62

【発明の名称】 不正アクセス判断装置及び方法

【請求項の数】 20

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士
通株式会社内

 【氏名】 藤井 勇作

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士
通株式会社内

 【氏名】 新崎 卓

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100079359

 【弁理士】

 【氏名又は名称】 竹内 進

 【電話番号】 03(3432)1007

【選任した代理人】

 【識別番号】 100093584

 【弁理士】

 【氏名又は名称】 宮内 佐一郎

 【電話番号】 03(3432)1007

【手数料の表示】

【予納台帳番号】 009287

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704823

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 不正アクセス判断装置及び方法

【特許請求の範囲】

【請求項 1】

サービス提供システムが利用者から受けた認証請求に基づく ID 情報及び生体情報を入力して記憶する記憶部と、

入力された ID 情報及び生体情報と過去に入力された ID 情報及び生体情報と比較照合する比較照合部と、

前記比較照合部の出力に基づき不正アクセス者による認証請求を判断して前記サービス提供システムに通知する制御部と、

を設けたことを特徴とする不正アクセス判断装置。

【請求項 2】

請求項 1 記載の不正アクセス判断装置に於いて、前記記憶部は、

サービス提供システムが利用者から受けた認証請求に基づく ID 情報及び生体情報を入力して一時記憶する入力記憶部と、

過去にサービス提供システムが利用者から受けた認証請求に基づく ID 情報及び生体情報を保存記憶する利用情報記憶部と、

を備えたことを特徴とする不正アクセス判断装置。

【請求項 3】

請求項 1 記載の不正アクセス判断装置に於いて、前記制御部は、前記比較照合部の出力により ID 情報が不一致で生体情報が一致する場合、或いは、ID 情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項 4】

請求項 1 記載の不正アクセス判断装置に於いて、

前記記憶部は、過去に入力した ID 情報及び生体情報に対応して送信元となる電話番号やネットワークアドレス等の端末位置及び入力時刻を記憶し、

前記制御部は、前記比較照合部による入力した ID 情報と同一端末位置から所定時間内に入力した過去の ID 情報と比較結果が不一致の場合、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項 5】

請求項 1 記載の不正アクセス判断装置に於いて、前記制御部は、入力した ID 情報に対し過去の ID 情報が連番になっているか否か判定し、連番を判定した際には所定回数目で不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項 6】

請求項 1 記載の不正アクセス判断装置に於いて、前記制御部は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致し ID 情報が異なる組合せを検出し、該組合せ数が所定数に達した時に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断装置。

【請求項 7】

請求項 1 記載の不正アクセス判断装置に於いて、前記比較照合部は、

入力した ID 情報と過去に入力した ID 情報とを比較して一致又は不一致を出力する ID 情報比較部と、

入力した生体情報と過去に入力した生体情報とを比較し、所定の一致度以上の値が得られた場合に生体情報の一致を出力し、所定の一致度未満の値が得られた場合に生体情報の不一致を出力する生体情報照合部と、
を備えた特徴とする不正アクセス判断装置。

【請求項 8】

請求項 1 記載の不正アクセス判断装置に於いて、更に時間を計測する時計部を設け、前記時計部で計測した時間情報に基づき、記憶されてから所定時間が経過した過去に入力した ID 情報及び生体情報を消去して比較照合の対象から除外することを特徴とする不正アクセス判断装置。

【請求項 9】

請求項 1 記載の不正アクセス判断装置に於いて、

前記記憶部は、過去に入力した ID 情報及び生体情報と共に送信元となる電話番号やネットワークアドレス等の端末位置を記憶し、

前記比較照合部は、入力した ID 情報及び生体情報を、同じ端末位置から過去に入力した ID 情報及び生体情報と比較照合することを特徴とする不正アクセス判断装置。

【請求項 10】

請求項 1 記載の不正アクセス判断装置に於いて、更に、

端末アドレス毎に認証請求の回数を記録する認証請求端末アドレス記録部と、

前記認証請求端末アドレスの参照により所定時間内に所定回数以上の認証請求が行われたことを検知し、前記比較照合部及び制御部を起動して不正アクセスを判断させる同一端末アクセス検知部と、

を設けたことを特徴とする不正アクセス判断装置。

【請求項 11】

サービス提供システムが利用者から受けた認証請求に基づく ID 情報及び生体情報を入力して記憶する記憶過程と、

入力された ID 情報及び生体情報と過去に入力された ID 情報及び生体情報と比較照合する比較照合過程と、

前記比較照合過程の出力に基づいて不正アクセス者による認証請求を判断して前記サービス提供システムに通知する制御過程と、
を設けたことを特徴とする不正アクセス判断方法。

【請求項 12】

請求項 11 記載の不正アクセス判断方法に於いて、前記記憶過程は、サービス提供システムが利用者から受けた認証請求に基づく ID 情報及び生体情報を入力して一時記憶する入力記憶過程と、過去にサービス提供システムが利用者から受けた認証請求に基づく ID 情報及び生体情報を保存記憶する利用情報記憶過程と、を備えたことを特徴とする不正アクセス判断方法。

【請求項 13】

請求項 11 記載の不正アクセス判断方法に於いて、前記制御過程は、前記比較照合過程の出力により ID 情報が不一致で生体情報が一致する場合、或いは、ID 情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項 14】

請求項 11 記載の不正アクセス判断方法に於いて、前記記憶過程は、過去に入力した ID 情報及び生体情報に対応して送信元となる電話番号やネットワークアドレス等の端末位置及び入力時刻を記憶し、前記制御過程は、前記比較照合過程による入力した ID 情報と同一端末位置から所定時間内に入力した過去の ID 情報と比較結果が不一致の場合、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項 15】

請求項 11 記載の不正アクセス判断方法に於いて、前記制御過程は、入力した ID 情報に対し過去の ID 情報が連番になっているか否か判定し、連番を判定した際には所定回数目で不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項 16】

請求項 11 記載の不正アクセス判断方法に於いて、前記制御過程は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致し ID 情報が異なる組み合わせを検出し、該組み合わせ数が所定数に達した時に、不正アクセス者による認証請求と判断することを特徴とする不正アクセス判断方法。

【請求項 17】

請求項 11 記載の不正アクセス判断方法に於いて、前記比較照合過程は、
入力した ID 情報と過去に入力した ID 情報とを比較して一致又は不一致を出力する ID 情報比較過程と、

入力した生体情報と過去に入力した生体情報とを比較し、所定の一致度以上の値が得られた場合に生体情報の一致を出力し、所定の一致度未満の値が得られた場合に生体情報の不一致を出力する生体情報照合過程と、
を備えたことを特徴とする不正アクセス判断方法。

【請求項 18】

請求項 11 記載の不正アクセス判断方法に於いて、更に時間を計測する時計過程を設け、前記時計過程で計測した時間情報に基づき、記憶されてから所定時間が経過した過去に入力した ID 情報及び生体情報を消去して比較照合の対象から除外することを特徴とする不正アクセス判断方法。

【請求項 19】

請求項 11 記載の不正アクセス判断方法に於いて、
前記記憶過程は、過去に入力した ID 情報及び生体情報と共に送信元となる電話番号やネットワークアドレス等の端末位置を記憶し、
前記比較照合過程は、入力した ID 情報及び生体情報を、同じ端末位置から過去に入力した ID 情報及び生体情報と比較照合することを特徴とする不正アクセス判断方法。

【請求項 20】

請求項 11 記載の不正アクセス判断方法に於いて、更に、
端末アドレス毎に認証請求の回数を記録する認証請求端末アドレス記録過程と、
前記認証請求端末アドレスの参照により所定時間内に所定回数以上の認証請求が行われたことを検知し、前記比較照合過程及び制御過程を起動して不正アクセスを判断させる同一端末アクセス検知過程と、
を設けたことを特徴とする不正アクセス判断方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、サービス提供システムに対するアタッカの不正なアクセスを判断する不正アクセス判断装置及び方法に関し、特に、ID 情報に指紋や虹彩等の生体情報を組み合わせてサービス提供システムに認証請求を行う際のアタッカの不正アクセスを判断する不正アクセス判断装置及び方法に関する。

【0002】

【従来の技術】

現在、通信回線のインフラが整いつつあり、コンピュータなどの情報機器が通信回線を介して相互に接続され、利用者は、遠隔地から様々なサービスを利用できるようになっている。

【0003】

このようなサービス提供システムでは、システム利用時、利用者が正規ユーザであるかどうかをパスワードを用いて確かめている。また近年では、指紋や虹彩などの生体情報を用いて、本人確認する技術が確立しつつあり、本人確認にこれらの生体情報照合を応用することが考えられる。

【0004】

【発明が解決しようとする課題】

しかしながら、このようなサービス提供システムにあっては、正規のユーザ以外に、悪意のある者が手軽に遠隔地から各種の情報機器に不正にアタックできる可能性がある。例えば、遠隔地から自分のコンピュータを使って自動的にパスワードを発見するプログラムを作成できるため、犯罪者にとっても犯罪しやすい環境が整いつつある。

【0005】

そこでシステムの利用するための認証請求に対する本人確認のため、IDコードに指紋や虹彩などの生体情報を組み合わせてセキュリティを高めているが、正規ユーザの生体情報を不正に入手できれば、IDコードを変えながら生体情報を連続入力するといった手法でアタックされる可能性がある。

【0006】

このため生体情報を個人認証に使用した場合にも、ますます、犯罪者からのアタックを意識したシステムを構築する必要がある。

【0007】

本発明は、認証請求にID情報と生体情報を使用したサービス提供システムに対し、正規ユーザになりすました不正アクセス者のアタックを監視判断してシステムを支援する不正アクセス判断装置及び方法を提供することを目的とする。

【0008】

【課題を解決するための手段】

図1は本発明の原理説明図である。

【0009】

本発明は、図1(A)のように、サービス提供システム10が利用者端末14から受けた認証請求に基づくID情報30及び生体情報32を入力して記憶する記憶部、記憶部に入力されたID情報及び生体情報と過去に入力されたID情報及び生体情報と比較照合する比較照合部、及び比較照合部の出力に基づいて不正アクセス者による認証請求を判断してサービス提供システム10に通知する制御部28とを設けたことを特徴とする。

【0010】

このように本発明は、ユーザがID情報と生体情報を用いてシステムに対し本人確認のための認証請求を行った際に、保存している過去に行われた認証要求のID情報と生体情報と比べ、アタッカによる不正なアクセスかどうかを推測判断することを基本とする。もし不正にシステムに侵入しようとしているアタッカからの攻撃の可能性があるかと判断した場合には、サービス提供システムに不正アクセスであることを通知し、サービス提供を拒否させることで侵入を防ぐ。

【0011】

ここで記憶部は、サービス提供システムが利用者から受けた認証請求に基づくID情報及び生体情報を入力して一時記憶する入力記憶部18、20と、図1(B)のように、過去にサービス提供システムが利用者から受けた認証請求に基づくID情報及び生体情報を保存記憶する利用情報記憶部22を備える。

【0012】

具体的に、アタッカの攻撃は、自分の生体情報や偽造した生体情報を使用し、これにID情報をランダムに組み合わせて認証請求を次々と発信してシステムに侵入しようとする。このためアタックの形態は、次の3つに分類できる。

【0013】

アタック形態1：生体情報を固定し、ID情報を次々と変えてアタックする。

【0014】

アタック形態2：ID情報を固定し、生体情報を次々と変えてアタックする。

【0015】

アタック形態2：③生体情報とID情報の両方を次々と変えてアタックする。

【0016】

本発明の制御部28は、これらアタック形態に対応する不正アクセスの判断ルールとして次のものを備える。

【0017】

[判断ルール1]

制御部28は、比較照合部の出力によりID情報が不一致で生体情報が一致している場合に、不正アクセス者による認証請求と判断する。これは、アタック形態1であり、アタッカが偽造した生体情報や自分の生体情報を使用し、複数利用

者のID情報に組み合わせて認証請求を行った場合である。例えば生体情報に指紋を用いている場合には、アタッカは、利用者のID番号を入力し、指を指紋スキャナに押すという動作を繰り返している。

【0018】

〔判断ルール2〕

制御部28は、比較照合部の出力によりID情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断する。これはアタック形態2であり、アタッカが偽造した生体情報や自分の生体情報を使用し、特定のID情報に組み合わせて認証請求を行った場合である。例えば生体情報に指紋を用いている場合には、アタッカは、同一のID番号を入力し、指を変えながら指紋スキャナに押すという動作を繰り返している。

【0019】

〔判断ルール3〕

制御部28は、比較照合部の出力によりID情報が不一致で生体情報が一致する場合、或いは、ID情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断する。これはアタック形態3であり、アタッカが偽造した生体情報や自分の生体情報を使用し、複数利用者のID情報に組み合わせて認証請求を行った場合である。例えば生体情報に指紋を用いている場合には、アタッカは、指を変えながら指紋スキャナに押すという動作を、利用者のID番号を変えながら繰り返している。

【0020】

〔判断ルール4〕

記憶部は、過去に入力したID情報及び生体情報に対応して、送信元となる電話番号やネットワークアドレス等の端末位置及び入力時刻を記憶し、制御部は、同一端末から新たに入力したID情報と、過去の所定時間内に同一端末から入力されたID情報と比較した結果が不一致の場合、不正アクセス者による認証要求と判断する。

【0021】

これはアタックは通常コンピュータを用いて、自動的に大量の認証請求を集中

して行うことに着目したものであり、過去に入力した生体情報との照合を行わずに不正使用の判断ができる。

【0022】

[判断ルール5]

制御部28は、入力したID情報に対し過去のID情報が連番になっているか否か判定し、連番を判定した際には所定回数目で不正アクセス者による認証請求と判断する。

【0023】

利用者のID情報が連番で続けて入力されている場合は、一層アタッカからの攻撃の可能性が高い。アタッカがコンピュータを使って順番に攻撃していることが考えられるからである。したがって、入力されるIDが連番であるかどうか調べると、アタッカからの攻撃であることの確信が持て、不正アクセスかどうかの確からしさが向上する。

【0024】

[判断ルール6]

制御部28は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致しID情報が異なる組合せを検出し、この組合せ数が所定数に達した時に、不正アクセス者による認証請求と判断する。

【0025】

一方、アタッカが不正にアクセスしようとしたのではなく、正規の利用者が単にID情報を入力し間違える場合もある。そこで所定の回数、例えば3回まではID情報を再入力できるようにし、ID情報の入力し間違いを不正アクセスと誤認することを回避する。

【0026】

比較照合部は、入力したID情報と過去に入力したID情報とを比較して一致又は不一致を出力するID情報比較部24と、入力した生体情報と過去に入力した生体情報とを比較し、所定の一致度以上の値が得られた場合に生体情報の一致を出力し、所定の一致度未満の値が得られた場合に生体情報の不一致を出力する生体情報照合部26とで、ID情報と生体情報の比較照合を個別にできるように

している。

【0027】

本発明の不正アクセス判断装置は、更に時間を計測する時計部を設け、時計部で計測した時間情報に基づき、記憶されてから所定時間が経過した過去に入力したID情報及び生体情報を消去して比較照合の対象から除外する。

【0028】

正規のユーザが不正にアクセスしようとしたのではなく、単にID情報を入力し間違える場合、いつまでもその事実を保存記憶しておく、正規のユーザ本人であるにも関わらず、不正アクセスと判定されてアクセスできない状況が発生し得る。そこで、記憶保存に時間制限を行って所定時間が経過したら消去し、不正アクセスと誤認される状況を回避する。

【0029】

一般的にアタッカは、短時間に集中的に攻撃を行うので、保存記憶に時間制限を行ってもアタッカの不正アクセスを判断するための保存記憶は十分に得られる。

このため正規のユーザが何回もID情報を入力し間違えても、システムを利用できる。更に、保存記憶の時間が制限されることで、過去に入力したID情報及び生体情報の記憶量が制限され、新たに入力したID情報及び生体情報との照合比較の負担が低減する。

【0030】

記憶部は、過去に入力したID情報及び生体情報と共に送信元となる電話番号やネットワークアドレス等の端末位置を記憶し、比較照合部は、入力したID情報及び生体情報を、同じ端末位置から過去に入力したID情報及び生体情報と比較照合する。

【0031】

アタッカは偽造した生体情報や自分の生体情報を用いて、特定の端末から総当たり攻撃を行ってくる場合がある。この場合、過去に入力されたID情報及び生体情報の全てと比較照合することは大きな負担になる。そこで、ID情報と生体情報の比較照合を行う端末を、現在、入力を行っている特定の端末に絞ることで

比較照合の負担を減らす。

【0032】

本発明の不正アクセス判断装置は、更に、不正アクセス者の情報を記録するログ記録部を設ける。ログ記録部には、不正アクセス者の生体情報、不正アクセス者の電話番号もしくはネットワークアドレス等の端末位置、及び不正アクセスの対象となったID情報の少なくともいずれかを記録する。

【0033】

ID情報に比べ生体情報は、盗むことが困難であることを考えると、用いられた生体情報はアタッカのものである確率が高く、これをロギングすることで犯罪装置の手掛かりとでき、不正アクセス者の特定や証拠に活用できる。

【0034】

また端末の位置や時間等を保存しておくことで、犯罪捜査の手掛かりとなる他、アタッカからの攻撃時にログ記録部を参照して端末を積極的に調べることができる。更に攻撃対象となったID情報の記録保存により、再攻撃に対してのセキュリティ対策に役立てることができる。

【0035】

本発明の不正アクセス判断装置は、更に、端末アドレス毎に認証請求の回数を記録する認証請求端末アドレス記録部と、認証請求端末アドレスの参照により所定時間内に所定回数以上の認証請求が行われたことを検知し、比較照合部及び制御部を起動して不正アクセスを判断させる同一端末アクセス検知部とを設ける。

【0036】

これは通常の業務では考えられないような同一端末からの認証請求の回数を検知した場合にのみ、ID情報と生体情報の比較照合に基づく不正アクセスの判断を起動するもので、不正判断の処理負担を減らすことができる。

【0037】

不正アクセス判断装置で使用する生体情報としては、指紋、声紋、虹彩パターン、網膜血管パターン、掌形、耳形、顔、署名等を用いる。これらの生体情報は

人に固有のものと仮定でき、ID情報が異なるのにも関わらず生体情報が同じであるということは発生しないと仮定して不正アクセスを判断する。

【0038】

制御部28は、不正アクセス者による認証請求を判断した際に、サービス提供システム10の管理者に判断結果を自動通知する。制御部28による管理者への自動通知は、固定電話、携帯電話、電子メール、専用通信回線、警告灯などを用いて通知する。

【0039】

アタッカからの攻撃であると判断された場合、その事実をシステム側からシステム管理者側に通知することで、システム管理者は、常にシステムを監視している必要はなく、管理者側の管理負担が軽減される。自動通知には広く普及している電話や電子メールを用いることで、コストが削減できる。

【0040】

更に、本発明は不正アクセス判断方法を提供するものであり、

サービス提供システムが利用者から受けた認証請求に基づくID情報及び生体情報を入力して記憶する記憶過程；

入力されたID情報及び生体情報と過去に入力されたID情報及び生体情報と比較照合する比較照合過程；

前記比較照合過程の出力に基づいて不正アクセス者による認証請求を判断して前記サービス提供システムに通知する判断制御過程；

を備える。この不正アクセス判断方法の詳細は、装置構成と基本的に同じになる。

。

【0041】

【発明の実施の形態】

図2は、本発明の不正アクセス判断装置の第1実施形態のブロック図である。

【0042】

図2において、本発明による不正アクセスの判断対象となるサービス提供システム10は、例えばインターネットやイントラネット等のネットワーク12を介

してユーザ端末 14 からのサービス要求を受け、ユーザが要求したサービスをオンラインで提供している。

【0043】

このようなサービス提供システム 10 はオンライン検索機能を備えたデータベースシステム等の適宜のサービスを提供するシステムであり、例えば百万人を越える膨大な数の正規ユーザが利用するシステム等である。

【0044】

このサービス提供システム 10 をユーザがユーザ端末 14 からのアクセスで利用する場合には、ユーザはサービス提供システム 10 側に予め登録された ID 情報 30 とユーザに固有の生体情報 (LB 情報) 32 を入力し、ユーザ端末 14 からネットワーク 12 を経由してサービス提供システム 10 に対し正規ユーザであることを確認するための認証請求 (本人確認の認証請求) を行う。

【0045】

この実施例において、ユーザが入力する生体情報 32 としては指紋を例に説明するが、これ以外に虹彩、声紋、網膜血管分布、署名等の生体情報を用いることができる。また生体情報の種類は、サービス提供システム 10 側に設けられている生体情報照合システムによって異なるが、例えば指紋なら指紋画像や指紋画像から抽出された生体キー情報を用いる。

【0046】

正規のユーザの ID 情報 30 及び生体情報 32 は、ユーザがサービス提供システム 10 の利用申込みを行った際に、サービス提供システム 10 側に予め登録されている。このため、ユーザが ID 情報 30 と生体情報 32 を入力してユーザ端末 14 からサービス提供システム 10 に対し認証請求を行うと、サービス提供システム 10 側において認証請求のあった ID 情報 30 に対応して予め登録している生体情報 32 を読み出し、入力した生体情報 32 と登録済みの生体情報を照合し、所定値以上の一致度が得られたときに生体情報は同じもの (照合一致) とし、認証請求のあったユーザ端末 14 に対しサービス提供システム 10 の利用を許可する。

【0047】

このような認証請求にID情報30と生体情報32の組合せを用いたサービス提供システム10に対し、アタッカによる不正アクセスを判断するため、本発明の不正アクセス判断システム16が支援装置として設けられている。不正アクセス判断システム16は、生体情報入力記憶部18、ID情報入力記憶部20、利用情報記憶部22、生体情報照合部24、ID情報比較部26及び制御部28で構成される。

【0048】

生体情報入力記憶部18とID情報入力記憶部20には、サービス提供システム10に対しユーザ端末14よりID情報30と生体情報32を使用した認証請求があった際に、サービス提供システム10に入力された生体情報32及びID情報30のそれぞれを一時的に入力記憶する。

【0049】

利用情報記憶部22には、サービス提供システム10に対するユーザ端末14からの認証請求で過去に入力されたID情報と生体情報がペアで記憶保存されている。

【0050】

図3は図2の利用情報記憶部22の記憶内容である。利用情報記憶部22は、ID情報記憶領域22-1と生体情報記憶領域22-2をもち、ID情報と生体情報をペアにして例えば(ID01, LB01)(ID05, LB05), ...のように保存記憶している。利用情報記憶部22の記憶領域は、例えば16進のアドレス0000~FFFFで決まるメモリ容量を持っており、このため最新に入力されたID情報と生体情報のペアを物理的なメモリ容量で決まる固定数分だけ記憶することになる。

【0051】

再び図2を参照するに、生体情報照合部24は、生体情報入力記憶部18に生体情報の入力記憶があったとき、利用情報記憶部22に保存記憶している過去に入力した生体情報との照合を行う。この生体情報の照合は、入力した生体情報と過去に入力した生体情報との一致度を求め、一致度が所定値以上であれば照合一致の出力を生じ、一致度が所定値未満であれば照合不一致の出力を生ずる。

【0052】

ID情報比較部26は、ID情報入力記憶部20にID情報が入力されると、利用情報記憶部22に保存記憶している過去に入力したID情報との比較を行い、一致または不一致の比較出力を生ずる。

【0053】

この生体情報照合部24とID情報比較部26による生体情報及びID情報の照合比較の処理は、サービス提供システム10に対するユーザ端末14からのID情報と生体情報の入力に基づくことから、同時に照合比較の処理動作が行われる。

【0054】

制御部28は、生体情報照合部24の照合結果とID情報比較部26の比較結果を受け取り、アタッカからの攻撃による不正アクセスかどうかを判断し、判断結果をサービス提供システム10に通知する。

【0055】

制御部28による不正アクセスの判断は、

①判断ルール1

比較照合結果に基づき、ID情報が不一致で生体情報が一致している場合に、不正アクセス者による認証請求と判断；

②判断ルール2

比較照合結果によりID情報が一致して生体情報が不一致の場合に不正アクセス者による認証請求と判断；

③判断ルール3

比較照合結果によりID情報が不一致で生体情報が一致する場合、あるいはID情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断；

の3つが基本的にある。

【0056】

図4は、判断ルール1に従って制御部28が判断する不正アクセスとそのときの利用情報記憶部22の記憶内容である。図4の不正アクセス25-1は、アタ

ツカが自分自身の指紋あるいは偽造した指紋による 1 つの生体情報 LB 1 を使って ID 情報を ID 1, ID 2, ID 3, ID 4 と変えながらアタックした場合である。具体的には、アタツカは正規ユーザの ID 番号を入力し、指を指紋スキャナに押す動作を繰り返している。

【0057】

このような不正アクセス 25-1 のアタツカによる不正な認証請求に対し、本発明の不正アクセス判断システム 16 の利用情報記憶部 22 には、不正アクセス 25-1 の入力時刻 $t_1 \sim t_4$ に対応して、入力した ID 情報と生体情報のペア (ID 1, LB 1) (ID 2, LB 1) (ID 3, LB 1) (ID 4, LB 1) が保存記憶される。

【0058】

ここでアタツカによる不正アクセス 25-1 は、時刻 $t_1 \sim t_4$ のように連続的に行われるが、その間に他の正規ユーザからの認証請求も受け付けることから、利用情報記憶部 22 には不正アクセス 25-1 に対応した保存記憶が図示のように離散的に行われることになる。

【0059】

このようなアタツカが 1 つの生体情報に複数の ID 情報を組み合わせて不正な認証請求を行った場合、本発明の制御部 28 にあっては判断ルール 1 を適用する。判断ルール 1 は比較照合結果に基づき、ID 情報が不一致で生体情報が一致している場合に、不正アクセス者による認証請求と判断する。この判断ルール 1 による図 4 の不正アクセス 25-1 に対する判断処理は次のようになる。

【0060】

まず時刻 t_1 の最初の不正アクセスの入力ペア (ID 1, LB 1) については、利用情報記憶部 22 の記憶保存ペアとの比較照合を行っても、該当するペアがないことから ID 情報及び生体情報の両方が不一致となる。

【0061】

次に時刻 t_2 で 2 回目の不正アクセスによる入力ペア (ID 2, LB 1) が入力すると、このとき時刻 t_1 の不正入力したペア (ID 1, LB 1) は利用情報記憶部 22 に既に保存記憶されているため、時刻 t_2 で入力した不正入力ペアと

時刻 t_1 で入力して既に保存している保存ペアとの比較照合により、ID 情報が不一致で生体情報が一致して判断ルール 1 の条件が成立する。

【0062】

したがって、時刻 t_2 で不正アクセスによるペア (ID2, LB1) が入力した時点で、本発明の制御部 28 は判断ルール 1 に従って不正アクセス者による認証請求と判断する。

【0063】

また時刻 t_3 の不正アクセスのペア (ID3, LB1) の入力については、利用情報記憶部 22 に時刻 t_1 , t_2 で保存した 2 つの保存ペア (ID1, LB1) (ID2, LB1) との間で、ID 情報が不一致で生体情報が一致する判断ルール 1 の条件が成立し、2 回分の不正アクセスが判断できる。

【0064】

更に時刻 t_4 の不正アクセスによるペア (ID4, LB1) の入力については、利用情報記憶部 22 の過去に入力した時刻 $t_1 \sim t_3$ の 3 つの保存ペアとの間の比較照合で 3 回分の不正アクセス者による認証請求が判断される。

【0065】

図 5 は、図 2 の制御部 28 による判断ルール 2 が適用される不正アクセスとそのときの利用情報記憶部 22 の内容である。判断ルール 2 は、比較照合結果により ID 情報が一致して生体情報が不一致の場合に不正アクセス者による認証請求と判断する。

【0066】

この判断ルール 2 は、アタッカが偽造した生体情報や自分の生体情報を使用し、特定の ID 情報に組み合わせて認証請求を行った場合を想定している。例えば、図 5 の不正アクセス 25-2 のように、アタッカが特定の ID 情報として ID1 を使用し、これにアタッカが自分の生体情報や偽造した生体情報 LB1, LB2, LB3, LB4 を組み合わせて認証請求を行った場合である。具体的には、アタッカは同一の ID 番号を入力し、指を変えながら指紋スキャナを押すというような動作を繰り返している。

【0067】

このようにアタッカがID情報を固定で生体情報を変えながら認証請求を行う不正アクセス25-2があると、これに対応して利用情報記憶部22には離散的に不正アクセスの入力ペアが保存記憶される。

【0068】

このような不正アクセス25-2について、判断ルール2による不正アクセスの判断は次のようになる。まず最初の時刻 t_1 の不正アクセスのペア(ID1, LB1)の入力にあっては、利用情報記憶部22には不正アクセスに対応する保存ペアはないため、ID情報及び生体情報の両方について比較照合結果が不一致となり、判断ルール2による不正アクセスは判断できない。

【0069】

次に時刻 t_2 で不正アクセス25-2によるペア(ID1, LB2)が入力すると、このとき利用情報記憶部22には時刻 t_1 に入力して保存された保存ペア(ID1, LB1)があるため、両者の比較照合によりID情報が一致して生体情報が不一致となる判断ルール2の条件が成立し、不正アクセス者による認証請求と判断する。

【0070】

不正アクセス25-2の時刻 t_3 , t_4 についても、それ以前に不正アクセスによる保存ペアがあることから、同様に判断ルール2に従って不正アクセス者による認証請求と判断し、時刻 t_3 の場合は不正アクセスの判断回数が2回分、時刻 t_4 にあっては3回分となる。

【0071】

図6は、図2の制御部28で不正アクセスを判断する判断ルール3の対象となる不正アクセスとそのときの利用情報記憶部22の説明図である。判断ルール3は、図4の判断ルール4と図5の判断ルール2が想定している不正アクセスが混在した場合に対応する。即ち判断ルール3は、比較照合結果によりID情報が不一致で生体情報が一致する場合、あるいはID情報が一致して生体情報が不一致の場合に、不正アクセス者による認証請求と判断する。

【0072】

図6の不正アクセス25-3は、アタッカが複数のID情報としてID1, I

D2, ID3 の例えば 3 つを準備し、更に生体情報として自分の指紋や偽造した指紋 LB1, LB2, LB3 の 3 つを準備し、これらを組み合わせたペアを使って時刻 $t_1 \sim t_9$ のように認証請求を行うアタックを行った場合である。

【0073】

このような不正アクセス 25-3 による認証請求の入力ペアがあった場合の判断ルール 3 による不正アクセスの判断は、次のようになる。

【0074】

まず時刻 $t_1 \sim t_3$ の不正アクセス 25-3 のペア (ID1, LB1) (ID2, LB2) (ID3, LB3) にあっては、それぞれの入力時点での利用情報記憶部 22 の保存ペアとの比較では ID 情報及び生体情報の両方について不一致となり、既に説明した判断ルール 1, 2 はもちろんのこと、この場合の判断ルール 3 による不正アクセスも判断できない。

【0075】

次に時刻 t_4 で、既に使用したが異なる組合せのペア (ID1, LB3) を不正アクセスで入力すると、このとき利用情報記憶部 22 に記憶している時刻 t_3 の保存ペア (ID3, LB3) と時刻 t_4 の入力ペア (ID1, LB3) との間で、既に説明した判断ルール 1 の「ID 情報が不一致で生体情報が一致する」の条件が成立し、不正アクセス者による認証請求と判断できる。

【0076】

同時に時刻 t_1 の保存ペア (ID1, LB1) と時刻 t_4 の入力ペア (ID1, LB3) との間で、既に説明した判断ルール 2 の「ID 情報が一致して生体情報が不一致」とする条件が成立し、同様に不正アクセス者による認証請求と判断できる。

【0077】

このように判断ルール 3 にあっては、不正アクセス 25-3 のような ID 情報と生体情報の両方を変えながらアタックが不正な認証請求を行った場合、ある入力時点で判断ルール 1 と判断ルール 2 の両方による不正アクセスの判断結果が同時に得られる。

【0078】

この点は時刻 t_5 , t_6 の不正アクセスの入力ペアについても同様である。更に時刻 $t_7 \sim t_9$ の不正アクセスの入力ペアについては、利用情報記憶部 22 の時刻 $t_1 \sim t_3$ と時刻 $t_4 \sim t_6$ の中に 2 個ずつ同じ ID 情報と生体情報が存在することから、例えば時刻 t_2 の不正アクセスによる入力ペア (ID1, LB2) については、判断ルール 1 と判断ルール 2 の各々による 2 回分の不正アクセスの判断結果が得られ、このため合計 4 つの不正アクセスの判断結果が同時に得られる。この点は時刻 t_8 , t_9 の不正アクセスの入力ペアについても同様である。

【0079】

ここで制御部 28 による 3 種類の不正アクセスに対する判断ルール 1～3 の使い方としては、生体情報が偽造しにくい場合についてはアタッカは同じ生体情報を使って ID 情報を変えてくることから、判断ルール 1 を使用すればよい。

【0080】

これに対し比較的偽造が容易な生体情報の場合については、ID 情報が一致して生体情報が不一致の場合に不正アクセスと判断する判断ルール 2 を適用すればよい。もちろん最も強力な判断ルールは、ID 情報及び生体情報の両方を変えてくる場合に対応した判断ルール 3 である。

【0081】

図 7 は、図 2 の不正アクセス判断システム 16 の第 1 実施形態における不正アクセス判断処理のフローチャートであり、制御部 28 の判断ルールとしては図 6 に示した判断ルール 3 を適用している。

【0082】

図 7 において、まずステップ S1 でサービス提供システム 10 に対するユーザ端末からの認証請求があると、この認証請求に伴って受信された ID 情報と生体情報がステップ S1 で取得され、生体情報入力記憶部 18 及び ID 情報入力記憶部 20 のそれぞれに記憶される。

【0083】

続いてステップ S2 で、入力記憶した生体情報と利用情報記憶部 22 に記憶保存している全ての生体情報を照合する。次にステップ S3 で、入力記憶した ID

情報と利用情報記憶部 22 に記憶保存している全ての ID 情報を比較する。このステップ S 2, S 3 の生体情報の照合及び ID 情報の比較による結果は制御部 28 に通知され、ステップ S 4, S 5 で判断ルール 3 に従った比較照合結果の判定が行われる。

【0084】

まずステップ S 4 は判断ルール 1 による判定であり、生体情報が一致し ID 情報の異なるものかどうかチェックする。このステップ S 4 の条件が成立すると、ステップ S 6 に進み、アタッカからの攻撃と判断してサービス提供システム 10 に通知する。

【0085】

またステップ S 5 で、判断ルール 2 に従った ID 情報が一致し生体情報の異なるものがあるか否かチェックする。このステップ S 5 の条件が成立すると、ステップ S 6 に進み、アタッカからの攻撃と判断してサービス提供システム 10 に通知する。一方、ステップ S 4 の判断ルール 1 の条件が成立し且つステップ S 5 で判断ルール 2 の条件も成立しなかった場合には、ステップ S 7 で正常利用と判断してシステムに通知する。

【0086】

本発明の不正アクセス判断システム 16 からアタッカからの攻撃である旨の通知を受けたサービス提供システム 10 は、そのとき入力している ID 情報と生体情報と予め登録している ID 情報の生体情報との間で照合一致が万が一得られていたとしても、例えばユーザ側に対し通常の認証以外の他のユーザ情報例えば生年月日等の入力を要求し、不正アクセスに対する防衛措置をとるようになる。

【0087】

また不正アクセス判断システム 16 から通知された不正アクセスの内容が、例えば図 6 の不正アクセス 25-3 のように明らかにアタッカによる攻撃であることが分かっている場合には、ユーザに対し警告を発してサービス提供を拒否する。即ちサービス提供システム 10 は、本発明による不正アクセス判断システム 16 から不正アクセス者による認証請求である旨の通知を受けることで、不正アクセスの内容に対応した適切な防衛措置を迅速にとることができる。

【0088】

ステップ S6 又はステップ S7 に続くステップ S8 にあっては、ステップ S1 で生体情報入力記憶部 18 及び ID 情報入力記憶部 20 に一時的に入力記憶した生体情報と ID 情報を、利用情報記憶部 22 に記憶して保存する。

【0089】

この場合、利用情報記憶部 22 が一杯であれば、最も古い保存ペアを証供してあらみたな入力ペアを記憶する。

【0090】

図 8 は、本発明の不正アクセス判断装置の第 2 実施形態のブロック図である。この第 2 実施形態にあっては、図 2 の不正アクセス判断システム 16 に更にログ記録部 34 を設けたことを特徴とする。それ以外の構成は図 2 の実施形態と同じである。

【0091】

ログ記録部 34 には、制御部 28 でアタッカからの攻撃による不正アクセスと判断された場合に、不正アクセス者の身元に関する情報を記録する。ログ記録部 34 に記録する情報としては

- ①不正アクセス時の生体情報
- ②不正アクセスの入力時刻
- ③不正アクセスの電話番号もしくはネットワークアドレス
- ④不正アクセスの対象となった ID 情報

等を記録する。ここで、不正アクセスを行ったユーザ端末の電話番号もしくはネットワークアドレスは、サービス提供システム 10 に設けているネットワーク通信部の例えばプロトコル層から収集することが可能である。

【0092】

図 9 は、図 8 の第 2 実施形態における不正アクセス判断処理のフローチャートである。図 9 において、ステップ S1～S6 の生体情報と ID 情報の入力記憶に対する保存情報との比較照合による不正アクセスの判断は、図 7 のフローチャートと同じであるが、ステップ S6 でアタッカからの攻撃と判断してサービス提供システム 10 に通知した後にステップ S7 で不正アクセスと判断されたとき、入

力記憶した生体情報と時間を例えばログ記憶部 34 に記憶している。

【0093】

このように図 8 の第 2 実施形態にあつては、ログ記録部 34 に不正アクセスと判断されたときの生体情報や時刻等を記録してアタッカ自身の身元情報を残しておくことにより、後の犯罪捜査でアタッカがだれであることを証明すること等が可能となる。

【0094】

図 10 は、本発明の不正アクセス判断装置の第 3 実施形態のブロック図である。この第 3 実施形態にあつては、図 8 の第 2 実施形態の不正アクセス判断システム 16 に、更に時計部 36 と電子メール発行部 38 を設けたことを特徴とし、それ以外の構成は図 2 の実施形態と同じである。

【0095】

時計部 36 は、時刻情報として「年、月、日、時、分」を計測して保持し、この時刻情報を利用情報記憶部 22 及び制御部 28 に通知する。制御部 28 は、時計部 36 からの時刻情報に基づいて利用情報記憶部 22 の保存内容を制御しており、記憶されてから所定時間を過ぎた ID 情報と生体情報の保存ペアを消去する。

【0096】

この結果、利用情報記憶部 22 には、入力してから一定時間内の過去に入力した ID 情報と生体情報のペアのみが保存記憶されていることとなり、ユーザ端末 14 からの認証請求に伴うサービス提供システム 10 からの生体情報及び ID 情報の入力を受けた際の生体情報照合部 24 及び ID 情報比較部 26 による過去の保存情報との照合比較の数を制限でき、不正アクセス判断システム 16 における判断処理の負担を軽減することができる。

【0097】

このように利用情報記憶部 22 に保存記憶する過去に入力した ID 情報と生体情報のペアを制限しても、通常、アタッカからの攻撃は短時間に連続して行われることが多いことから、アタッカによる不正アクセスを判断する上で支障は起きない。

【0098】

更に図10の第3実施形態にあっては、電子メール発行部38を設けたことで、制御部28は、アタッカからの攻撃による不正アクセスと判断した場合、アタッカによる不正アクセスがあった事実を電子メール発行部38に通知する。

【0099】

電子メール発行部38は、サービス提供システム10がアタッカに攻撃された事実を知らせる電子メールを作成し、メールシステム40に作成した電子メールを投函し、LANやWAN等のネットワークを経由してシステム管理者端末44に電子メールを送信する。これによってシステム管理者は、サービス提供システム10に対しアタッカによる攻撃があったことを直ちに知ることができる。

【0100】

このためシステム管理者44は、サービス提供システム10のログをチェックするなどして常に不正アクセスに対するシステムの状態を監視する必要がなくなり、システム管理者の負担を大幅に軽減し、且つアタッカの攻撃に対しシステム管理者は直ちに適切な対応策をとることができる。

【0101】

図11は、図10の利用情報記憶部22の記憶内容であり、ID情報記憶領域22-1、生体情報記憶領域22-2に加え、時刻情報記憶領域22-3を設けており、時刻情報記憶領域22-3には例えばアドレス「0000h」のように、「年、月、日、時、分」である9809170935が格納されている。

【0102】

制御部28は、このような利用情報記憶部22にID情報と生体情報のペアと共に記憶された時刻情報を利用して、記憶から所定時間を過ぎた保存ペアを消去する記憶制御を行っている。

【0103】

例えば現在時刻を t_n とし、このときアドレス「8000h」に保存記憶が行われたとすると、制御部28は例えば所定時間 $T=60$ 分を記憶保存時間として設定しており、現在時刻 t_n より所定時間 $T=60$ 分前がアドレス「0001h」の時刻 t_{n-1} の記憶内容であったとすると、それ以前のアドレス「0000

h」の時刻 t_{n-2} の記憶内容を消去する。

【0104】

この結果、利用情報記憶部22には現在時刻 t_n から $T=60$ 分の間に記憶されたID情報と生体情報のペアが時刻情報と共に保存されるだけであり、利用情報記憶部22の保存記憶量を不正アクセスに必要な適正量に制限し、入力した生体情報とID情報と、利用情報記憶部22に保存記憶された生体情報とID情報との比較照合の処理負担を低減することができる。

【0105】

図12は、図10の第3実施形態における不正アクセス判断処理のフローチャートである。図12において、ステップS1～ステップS6までの入力記憶した生体情報とID情報を保存記憶した生体情報とID情報と比較照合して不正アクセスかどうか判断する処理は、図9の第2実施形態のフローチャートと同じである。

【0106】

これに対し不正アクセスと判断してステップS6でサービス提供システム10にアタッカからの攻撃である旨を通知した場合、ステップS7で制御部28は電子メール発行部38にアタッカに攻撃された事実を通知し、システム管理者44に対し電子メールを発行する。

【0107】

更に次のステップS9において、制御部28は時計部36から与えられた現在時刻の時刻情報と図11のように利用情報記憶部22に記憶している時刻情報を用いて、記憶されてから所定時間が経過した生体情報とID情報の保存ペアを消去する。

【0108】

この保存記憶の消去が済んだ後、ステップS10で、そのとき生体情報入力記憶部18及びID情報入力記憶部20に一時的に入力記憶している入力したID情報と生体情報のペアを、時計部36から得られている時刻情報と共に利用情報記憶部22に記憶して保存する。

【0109】

図 13 は、本発明の不正アクセス判断装置の第 4 実施形態のブロック図である。この第 4 実施形態にあつては、図 10 の第 3 実施形態に対し更に、端末アドレス記憶部 48 と同一端末アクセス検知部 50 を設けている。また図 10 の電子メール発行部 38 に代えて、アラーム信号発行部 54 を設けている。それ以外の点は図 10 の第 3 実施形態と同じである。

【0110】

端末アドレス記憶部 48 は、サービス提供システム 10 に対しユーザ端末 14 より ID 情報と生体情報のペアを使用した認証請求があつた際に、認証請求を行ったユーザ端末 14 の電話番号やネットワークアドレスを記憶する。

【0111】

このユーザ端末 14 が認証請求を行ったときの電話番号やネットワークアドレスは、サービス提供システム 10 に設けているネットワーク通信部 52 から得られる。具体的には、ネットワーク通信部 52 のプロトコル層における受信パラメータとして電話番号やネットワークアドレスを取得することができる。

【0112】

図 14 は、図 13 の端末アドレス記憶部 48 の記憶内容を利用情報記憶部 22 と共に示している。図 14 の端末アドレス記憶部 48 は、図 6 の不正アクセス 25-3 のように、アタッカが ID 情報と生体情報の両方を変えながら攻撃した場合のアタッカが使用したユーザ端末の端末アドレスを時刻 $t_1 \sim t_5$ について記憶したもので、同じ端末アドレス A1 が記憶されている。

【0113】

また利用情報記憶部 22 には、図 6 の不正アクセス 25-3 の時刻 $t_1 \sim t_6$ の不正アクセスによる ID 情報と生体情報の入力ペアに対応した保存ペアが、時刻情報 $t_1 \sim t_5$ と共に記憶されている。

【0114】

再び図 13 を参照するに、同一端末アクセス検知部 50 は、端末アドレス記憶部 48 を参照し、「所定時間内に同一端末位置から所定回数以上の認証請求がある」の条件が成立するか否か検知する。この条件成立を検知すると、制御部 28 に対し不正アクセス判断のための処理要求を行う。

【0115】

例えば図14の端末アドレス記憶部48を例にとると、同一端末アクセス検知部50は新たな認証請求の入力時刻から過去所定時間 T_1 、例えば $T_1 = 15$ 分以内に、同一端末アドレスから所定回数 N 回以上例えば $N = 5$ 回以上の認証請求があったか否かチェックしている。

【0116】

この場合、入力時刻 t_5 の時点で過去 $T_1 = 15$ 分以内に同じ端末アドレス A_1 より5回の認証請求があることから、このとき同一端末アクセス検知部50は制御部28に対し不正アクセスの判断処理を要求する。

【0117】

このため制御部28は、生体情報照合部24及びID情報比較部26を起動し、時刻 t_5 の入力ペア(ID2, LB2)を、それまでに記憶している保存ペアと比較照合する。この場合、利用情報記憶部22に示している時刻 t_1 , t_2 , t_3 , t_4 の保存ペアとの間で、図6の判断ルールが成立して不正アクセス者による認証請求であることが判断される。

【0118】

ここで、同一端末アクセス検知部50で同一端末からの認証請求の回数 N を判断するための一定時間 T_1 は、アタッカによる攻撃が短時間に連続して行われることから、長くても30分から1時間程度の時間で十分である。

【0119】

また同一端末からのアクセス回数 N としては $N = 5$ 回を例にとっているが、正規のユーザによるID情報の入力ミスによるやり直しを何回許容するかによって、不正アクセスの処理要求を行う同一端末アクセスからのアクセス回数 N を決めればよい。例えば図14の場合には、 $N = 5$ 回で不正アクセスの判断要求を行っていることから、4回までは正規ユーザによるID情報の入力ミスによるやり直しを許容していることになる。

【0120】

再び図13を参照するに、アラーム信号発生部54は制御部28で不正アクセス者による認証請求と判断された場合、アタッカによる攻撃が行われた事実をシ

システム管理者に知らせるため、アラーム信号をネットワーク42を経由してシステム管理者端末44に通知してアラームを出させる。

【0121】

更に、この場合、ログ記録部32は制御部28で不正アクセス者による認証請求と判断されたときの生体情報入力記憶部18及びID情報入力記憶部20に一時記憶されている生体情報及びID情報の他に、端末アドレス記憶部48からユーザ端末の電話番号やネットワークアドレスを記録し、更に時計部36からの時刻情報も記録する。

【0122】

図15は、図13の第4実施形態による不正アクセス判断処理のフローチャートである。図15において、ステップS1でサービス提供システム10がユーザ端末14から受信した生体情報とID情報を取得して、生体情報入力記憶部18及びID情報入力記憶部20にそれぞれ入力記憶し、更に端末アドレス記憶部48にそのときネットワーク通信部52から得られた例えばユーザ端末14のネットワークアドレスを記録する。

【0123】

次にステップS2で、同一端末アクセス検知部50が端末アドレス記憶部48を参照し、同一端末から所定時間内に所定回数以上の利用要求即ち認証請求があったか否かチェックする。このステップS2の条件が得られると、ステップS3～S7、S9のように、図3の実施形態と同様な不正アクセスの判断処理が行われる。

【0124】

そしてステップS7で不正アクセス者の認証請求を判断してサービス提供システムにアタッカからの攻撃を通知した後、ステップS8でアラーム信号発生部54からシステム管理者44にアラーム信号を発行し、サービス提供システム10に対しアタッカから攻撃があったことを知らせる。

【0125】

続いてステップS10で利用情報記憶部22の記憶から一定時間過ぎた保存内容を消去した後、ステップS11で、このとき入力記憶した生体情報とID情報

のペアを時刻情報と共に記憶して、このときの認証請求に伴う一連の処理を終了する。

【0126】

次に本発明の不正アクセス判断システム 16 の制御部 28 において、不正アクセスを判断するための判断ルール 4, 5, 6 を説明する。

【0127】

図 16 の不正アクセスの判断処理は、判断ルール 4 を使用した場合である。判断ルール 4 は、同一端末について新たに入力した ID 情報と過去の所定時間内に入力した ID 情報とを比較した結果が不一致の場合、不正アクセス者による認証請求と判断する。

【0128】

この判断ルール 4 の特徴は、生体情報の照合を行っていない点である。このように生体情報の照合を行わずに ID 情報から不正アクセスを判断することで、不正アクセス判断処理の負担を大幅に減らすことができる。

【0129】

アタッカによる攻撃の中には、図 4 の不正アクセス 25-1 に示したように、特定のユーザ端末から生体情報を変えずに ID 情報を変えながら連続的に攻撃するパターンがある。この図 4 の不正アクセス 25-1 のような攻撃パターンについては、生体情報は同じであることから、過去に入力した生体情報と比較せず、ID 情報の変化のみを捉えることで、アタッカによる攻撃と判断することができる。

【0130】

この図 16 に適用される判断ルール 4 は、図 13 の第 4 実施形態のように、端末アドレス記憶部 48 に認証請求を行ったユーザ端末の電話番号やネットワークアドレス等が記憶されている場合に有効である。

【0131】

図 16 の判断ルール 4 を適用した不正アクセス判断処理を説明すると次のようになる。まずステップ S1 で、サービス提供システム 10 が受信した生体情報と ID 情報を取得して生体情報入力記憶部 18 及び ID 情報入力記憶部 20 に記憶

し、更にネットワーク通信部 52 から端末アドレス例えばネットワークアドレスを取得して端末アドレス記憶部 48 に記憶する。

【0132】

次にステップ S2 で同一端末から所定時間内に送られた ID 情報同士を照合する。この場合、図 14 のように、端末アドレス記憶部 48 において、例えば現在時刻 t_5 を基準に所定時間 $T = 15$ 分前までの同一端末アドレス A1 に対応する利用情報記憶部 22 の ID 情報を参照する。

【0133】

このときのアタックは図 4 の不正アクセス 25-1 のようなパターンを想定していることから、同一端末アドレス A1 の所定時間 T1 で利用情報記憶部 22 から得られる ID 情報は ID1, ID2, ID3, ID4, ... というように異なっている。

【0134】

そこでステップ S3 で ID 情報が不一致か否かチェックし、不一致であればステップ S4 に進み、アタッカからの攻撃と判断してサービス提供システム 10 に通知する。それ以降の処理は図 15 のステップ S8, 9 以降と同じである。

【0135】

図 17 は、例えば図 14 の第 4 実施形態の制御部 28 に判断ルール 5 を適用した場合の不正アクセス判断処理のフローチャートである。

【0136】

判断ルール 5 は、入力した ID 情報に対し過去の ID 情報が連番となっているか否か判定し、連番を判定した際には所定回数まで不正アクセス者による認証請求と判断する。

【0137】

新たな ID 情報の入力記憶を受けた際に、過去に入力した ID 情報を参照して連番となっている場合には、一層アタッカからの攻撃である可能性が高い。これはアタッカがコンピュータを使用して ID 番号を順番に変えながら攻撃していることが考えられるからである。したがって、判断ルール 5 によって入力される ID 番号が連番であるかどうかを調べるとアタッカからの攻撃であることの確信が

持て、これによって不正アクセスかどうかの確からしさが更に向上する。

【0138】

図17の判断ルール5を適用した不正アクセス判断処理を説明すると次のようになる。まずステップS1でサービス提供システム10が受信した生体情報とID情報を取得して入力記憶する。次にステップS2で、入力記憶したID情報と利用情報記憶部22に保存記憶している過去に連続入力した所定数のID情報を比較する。

【0139】

ステップS3でID情報が連番か否かチェックし、連番であれば、ステップS4で不正アクセス者によるアタッカからの認証請求による攻撃と判断し、サービス提供システム10に通知する。ステップS5以降は図16と同じである。

【0140】

図18は、図13の第4実施形態の制御部28の不正アクセスの判断に適用される判断ルール6を用いたフローチャートである。

【0141】

判断ルール6は、入力した生体情報と過去に入力した生体情報が一致した際に、生体情報が一致しID情報が異なるそれ以外の組合せを検出し、この組合せ数が所定数に達したときに不正アクセス者による認証請求と判断する。

【0142】

この判断ルール6は、図4に示した判断ルール1の変形と言える。即ち図4の判断ルール1にあっては、生体情報が一致しID情報が不一致とする条件が1つでも成立すると不正アクセス者による認証請求と判断している。これに対し判断ルール6は、判断ルール1の条件が所定数以上となったときに不正アクセス者による認証請求と判断する。

【0143】

この判断ルール6は、アタッカが不正にアクセスしようとしたのではなく、正規のユーザが単にID情報を入力し間違えた場合に、誤って不正アクセス者による認証請求と判断してしまうことを回避するためである。

【0144】

具体的には、図4の不正アクセス25-1がアタッカによるものではなく正規のユーザがID情報の入力ミスをして、やり直した場合であるとする。この場合、例えば不正アクセスと判断するID番号の相違回数をN回に設定していたとすると、正規ユーザはN+1回までID情報の入力ミスが許容される。例えば不正アクセスと判断するID情報の不一致数をN=3回に設定していたとすると、正規ユーザはN+1=4回の入力ミスが許容できる。

【0145】

このため図4の不正アクセス25-1のように、ユーザが4回連続してID情報の入力ミスを行ったとすると、これに対応した利用情報記憶部22の保存記憶からID情報の不一致数は時刻t1では0回、時刻t2では1回、時刻t3では2回、時刻t4では3回であり、この時点まで正規ユーザの入力ミスが許容される。もう1回ID情報の入力を誤ると、そのときの利用情報記憶部22の保存ID情報に基づく不一致数は4回となり、この時点で不正アクセス者による認証請求と判断される。

【0146】

この判断ルール6を適用した不正アクセス判断処理を図18のフローチャートについて説明すると、次のようになる。まずステップS1でサービス提供システム10が受信したユーザの認証請求に伴う生体情報とID情報を取得して入力記憶し、ステップS2で、入力記憶した生体情報と過去の全ての生体情報を照合し、ステップS3で生体情報が一致しID情報が異なるものがあるか否かチェックする。

【0147】

この条件を満足するものがあればステップS4に進み、該当する組合せは予め定めたN個以上か否かチェックする。N個未満であれば正規ユーザによるID情報の間違いによる再入力と判断し、ステップS7で正常利用と判断してシステムに通知する。

【0148】

N個以上であった場合にはステップS5に進み、アタッカからの攻撃と判断してサービス提供システムに通知し、更にステップS6でシステム管理者にアラ-

ム信号を発行する。ステップS8、S9は図17のステップS7、S8と同じである。

【0149】

尚、上記の実施形態は、制御部における不正アクセスの判断に判断ルール1～6を個別に適用する場合を例にとっているが、これらの判断ルールを適宜に組み合わせ不正アクセスを判断するようにしてもよい。

【0150】

また上記の実施形態は、生体情報として指紋を例にとるものであったが、これ以外の生体情報である声紋、虹彩パターン、網膜血管パターン、掌形、耳形、顔等の各個人特有の生体情報についても全く同様に不正アクセスを判断することができる。

【0151】

更に本発明は、その目的と利点を損なわない範囲の適宜の変形を全て含む。更にまた本発明は、上記の実施形態で示した数値による限定は受けない。

【0152】

【発明の効果】

以上説明してきたように本発明によれば、サービス提供システムに入力される認証請求のための利用者のID番号と生体情報のペアについて、過去に入力されたID情報と生体情報の保存ペアと比べることで、アタッカによる不正アクセスの攻撃が行われているかどうかを推測判断し、アタッカからの攻撃の可能性があると判断した場合には、攻撃対象となっているサービス提供システムにアタッカからの攻撃が行われていることを通知して適切な防衛対策をとらせることができる。

【0153】

また生体情報は個人固有のものなので、不正アクセスと判断した際に、アタッカの身元情報をロギングしていくことで、次のアタッカの攻撃に対する対抗措置や後の犯罪捜査での有効な手掛かりを与えることができ、多数のユーザからのアクセスに対しサービスを提供するシ

システムのセキュリティを大幅に高めることができる。

【0154】

尚、本発明の不正アクセス判断装置に於いて、その制御部は、不正アクセス者による認証請求を判断した際に、サービス提供システムの管理者に判断結果を自動通知することを特徴とする。

【0155】

また本発明の不正アクセス判断方法に於いて、その制御過程は、不正アクセス者による認証請求を判断した際に、サービス提供システムの管理者に判断結果を自動通知することを特徴とする。

【図面の簡単な説明】

【図 1】

本発明の原理説明図

【図 2】

認証請求の入力情報と過去の入力記憶の全てを比較照合して不正アクセスを判断する本発明の第 1 実施形態のブロック図

【図 3】

固定記憶容量をもつ図 2 の利用情報記憶部の説明図

【図 4】

生体情報を固定し ID 情報を変えた判断ルール 1 が適用される不正アクセスと利用情報記憶部の説明図

【図 5】

ID 情報を固定し生体情報を変えた判断ルール 2 が適用される不正アクセスと利用情報記憶部の説明図

【図 6】

ID 情報と生体情報の両方を変えた判断ルール 3 が適用される不正アクセスと利用情報記憶部の説明図

【図 7】

図 2 の不正アクセス判断処理のフローチャート

【図 8】

不正アクセス者の身元情報を記憶するロギング機能を備えた本発明の第 2 実施形態のブロック図

【図 9】

図 8 の不正アクセス判断処理のフローチャート

【図 10】

時間計測機能とシステム管理者への自動通報機能を備えた本発明の第 3 実施形態のブロック図

【図 11】

図 10 の利用情報記憶部の説明図

【図 12】

図 10 の不正アクセス判断処理のフローチャート

【図 13】

端末アドレスの記憶機能を備えた本発明の第 3 実施形態のブロック図

【図 14】

図 13 の端末アドレス記憶部と利用情報記憶部の説明図

【図 15】

同一端末から所定時間内に所定回数の認証請求があったときに起動する図 14 の不正アクセス判断処理のフローチャート

【図 16】

同一端末から所定時間内に入力した ID 情報のみにより不正アクセスを判断する判断ルール 4 が適用される図 14 の不正アクセス判断処理のフローチャート

【図 17】

ID 情報の連番入力から不正アクセスを判断する判断ルール 5 が適用される図 14 の不正アクセス判断処理のフローチャート

【図 18】

ID 情報につき正規ユーザによる誤入力と不正アクセスによる入力を区別する判断ルール 6 が適用される図 14 の不正アクセス判断処理のフローチャート

【符号の説明】

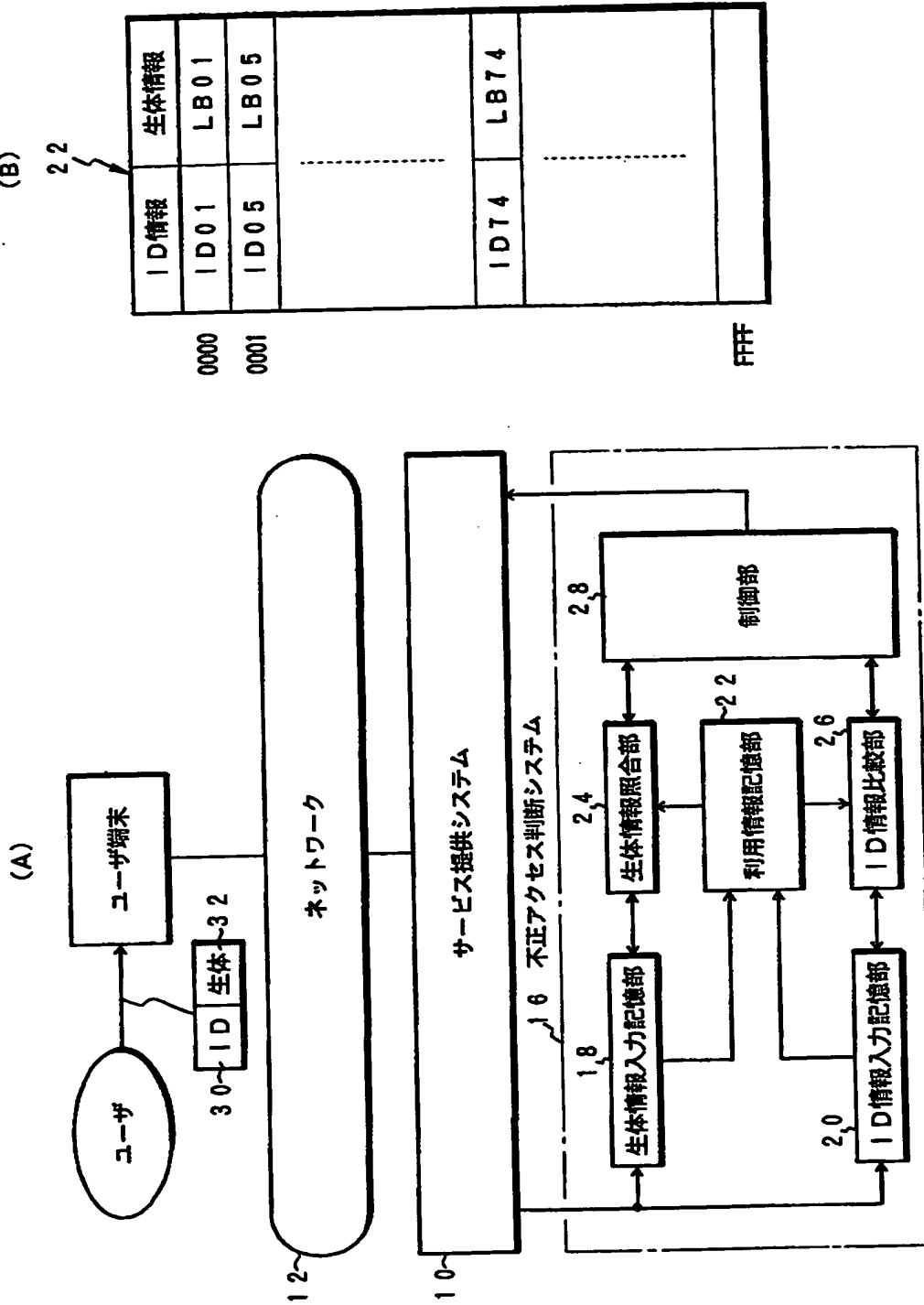
- 10：サービス提供システム
- 12, 42：ネットワーク（LAN/WAN）
- 14：ユーザ端末
- 16：不正アクセス判断システム
- 18：生体情報入力記憶部
- 20：ID情報入力記憶部
- 22：利用情報記憶部
- 24：生体情報照合部
- 25-1：不正アクセス（アタック1）
- 25-2：不正アクセス（アタック2）
- 25-3：不正アクセス（アタック3）
- 26：ID情報比較部
- 28：制御部
- 30：ID情報
- 32：生体情報
- 34：ログ記憶部
- 36：時計部
- 38：電子メール発行部
- 42：メールシステム
- 44：システム管理者
- 46：時刻情報
- 48：端末アドレス記憶部
- 50：同一端末アクセス検知部
- 52：ネットワーク通信部

【書類名】

図面

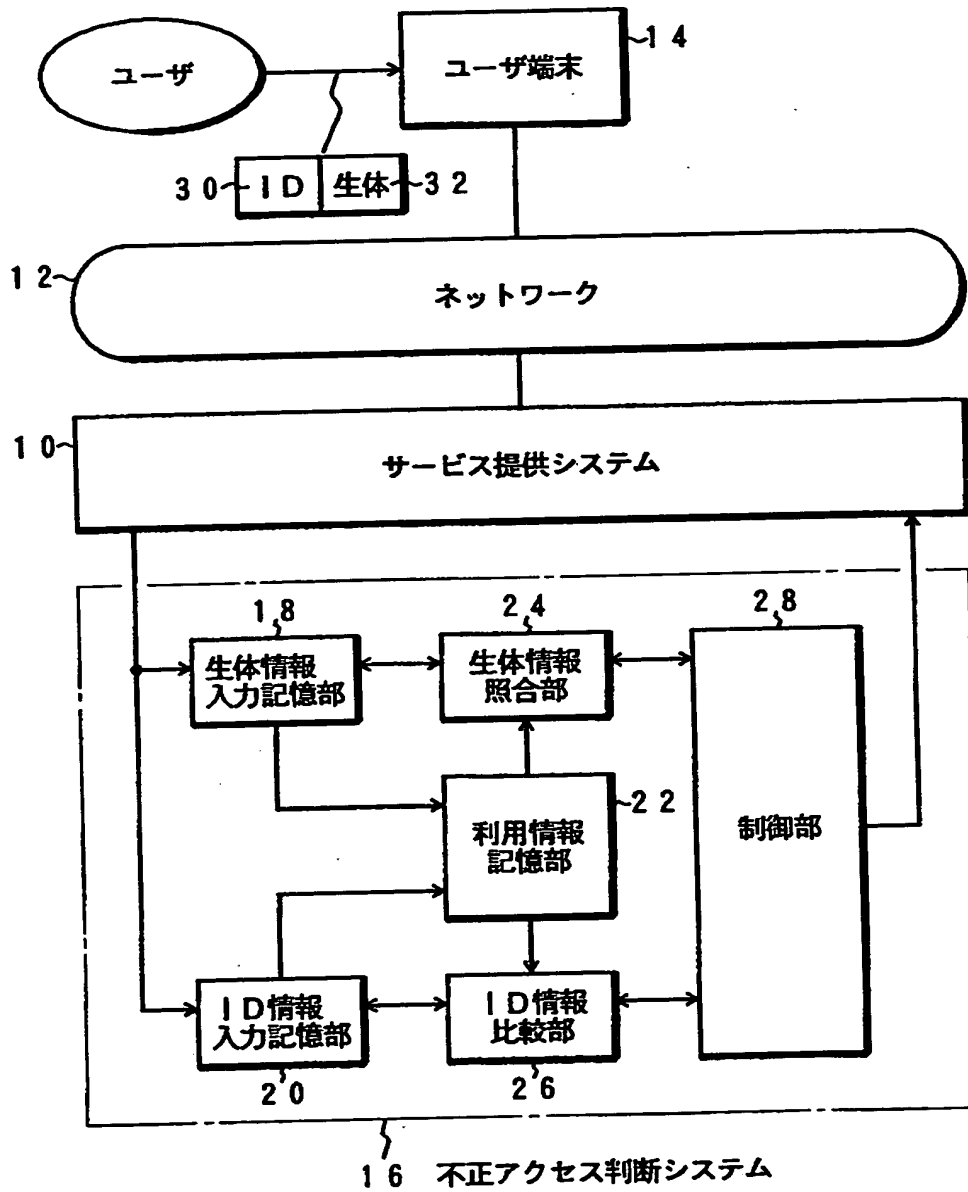
【図 1】

本発明の原理説明図



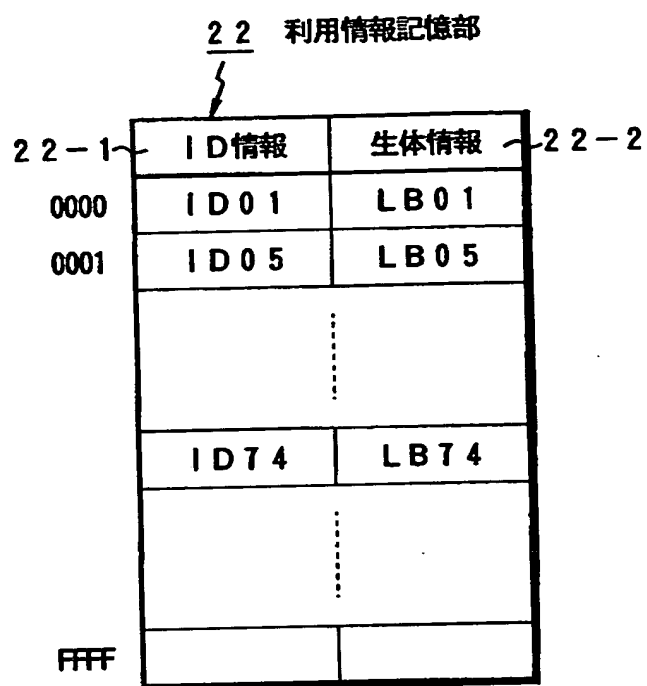
【図 2】

認証請求の入力情報と過去の入力記憶の全てを比較照合して不正アクセスを判断する本発明の第 1 実施形態のブロック図



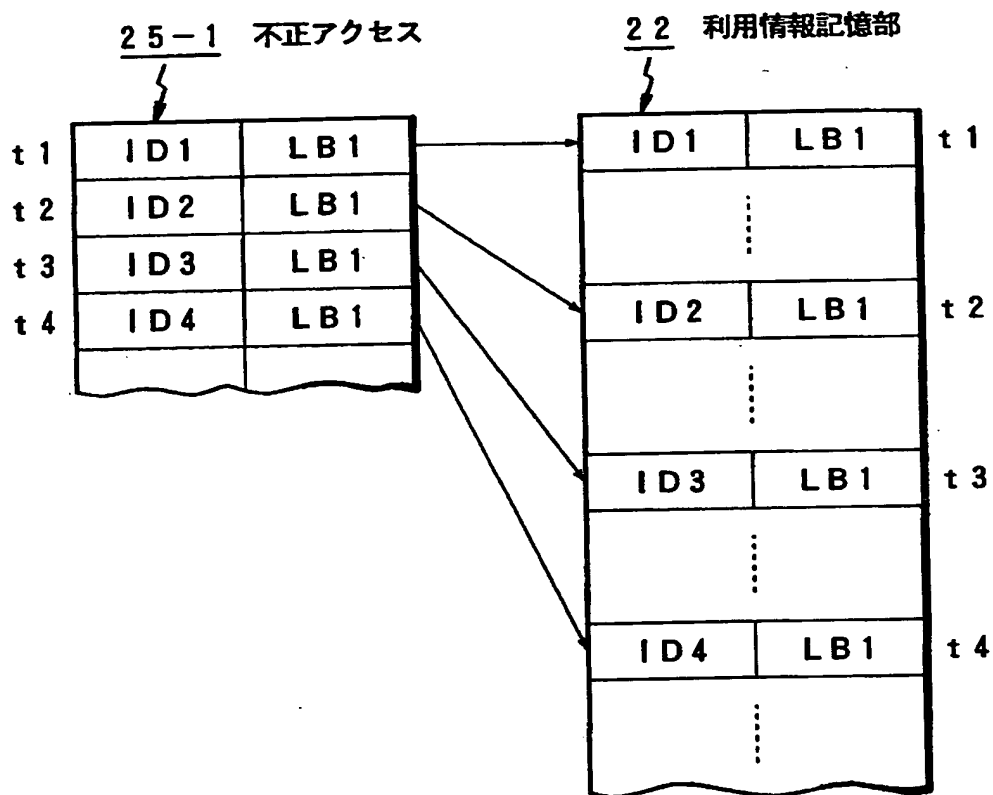
【図 3】

固定記憶容量をもつ図 2 の利用情報記憶部の説明図



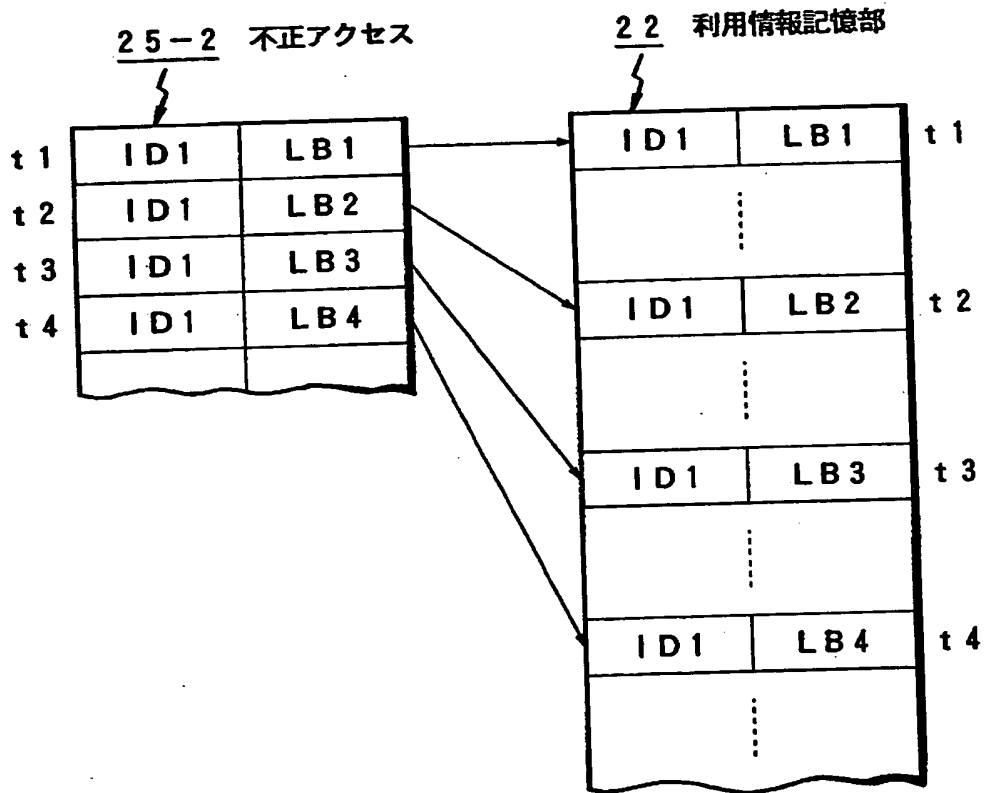
【図 4】

生体情報を固定し ID 情報を変えた判断ルール 1 が適用される不正アクセスと
利用情報記憶部の説明図



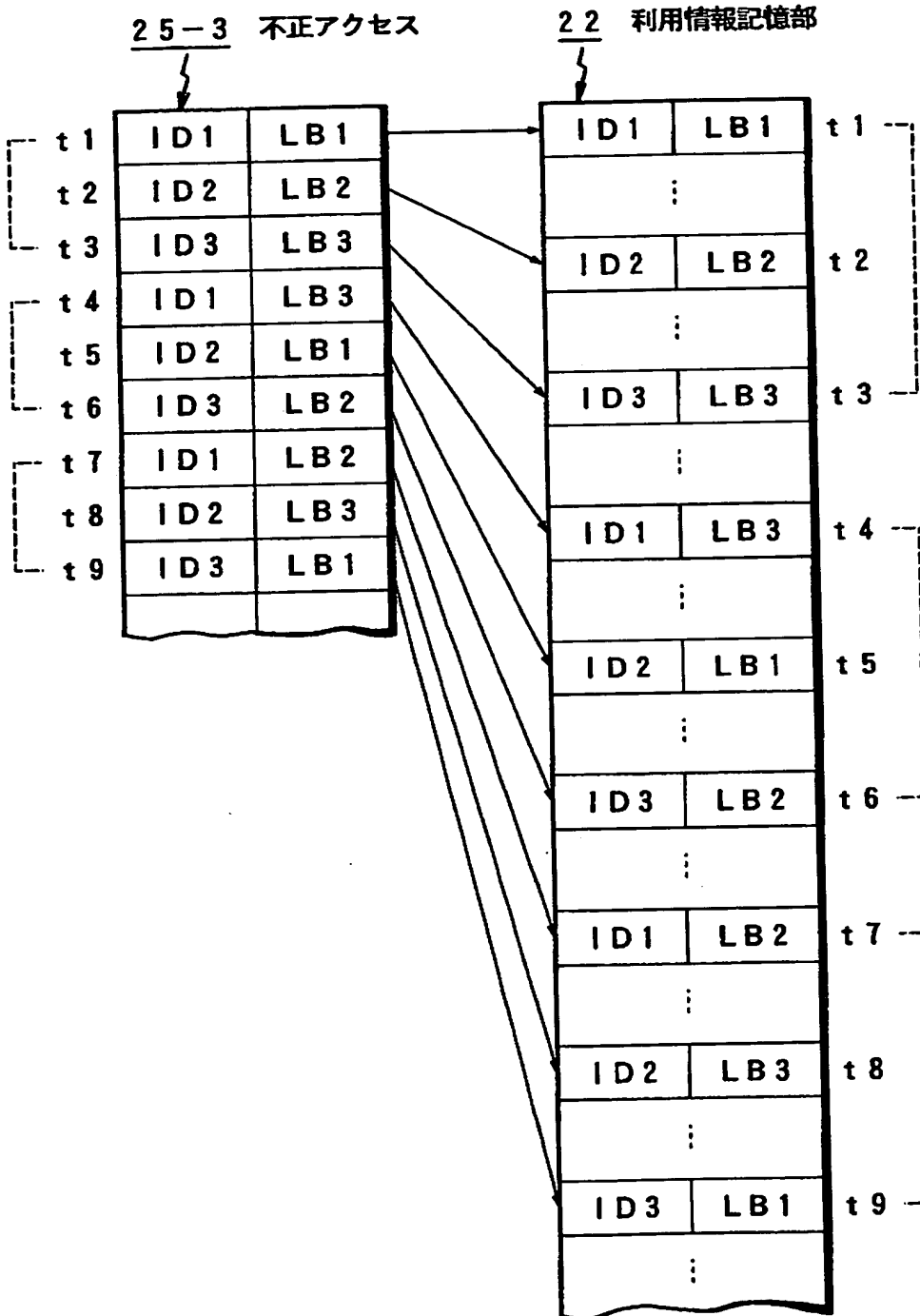
【図 5】

！ ID情報を固定し生体情報を変えた判断ルール2が適用される不正アクセスと
利用情報記憶部の説明図



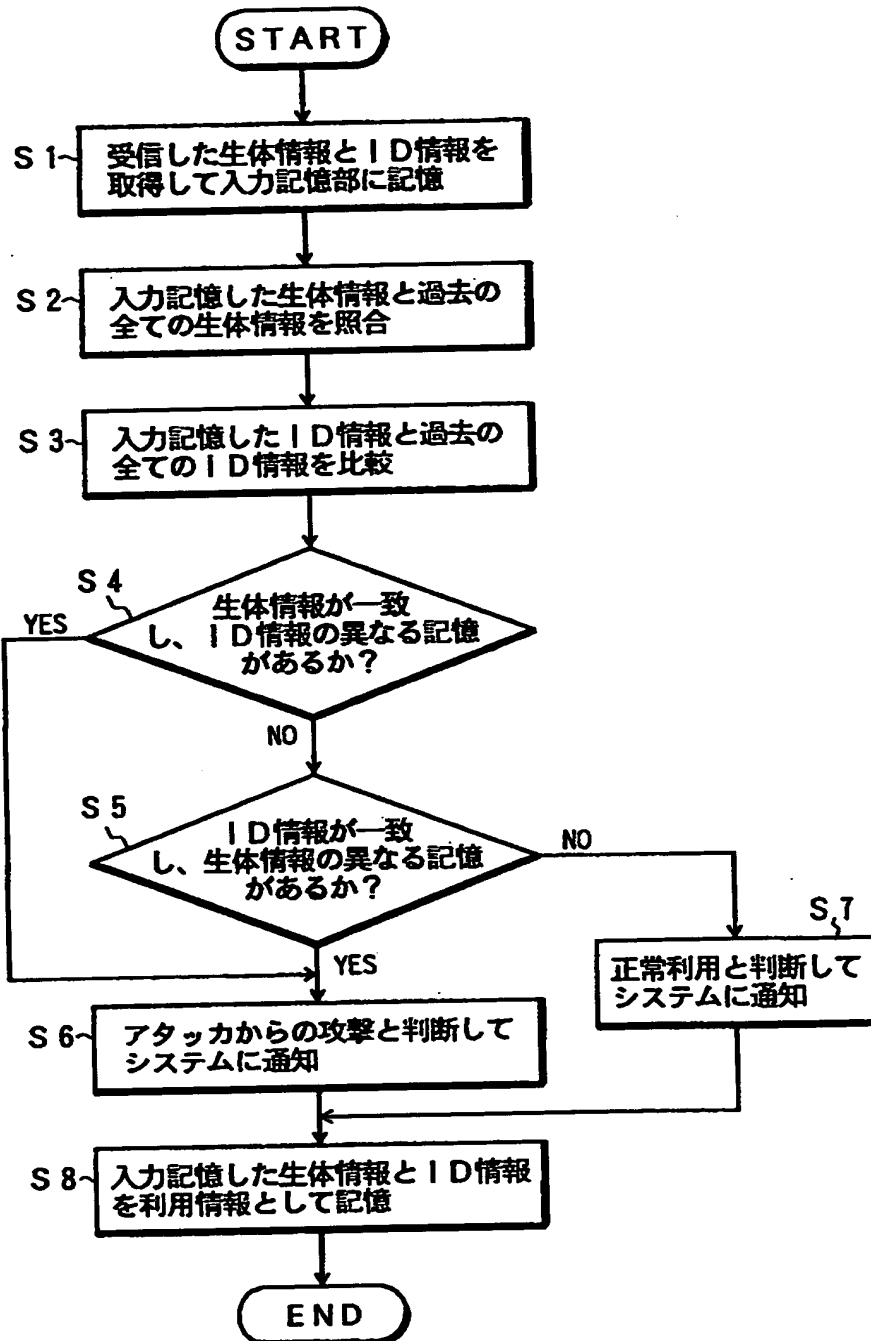
【図 6】

ID情報と生体情報の両方を変えた判断ルール3が適用される不正アクセスと
利用情報記憶部の説明図



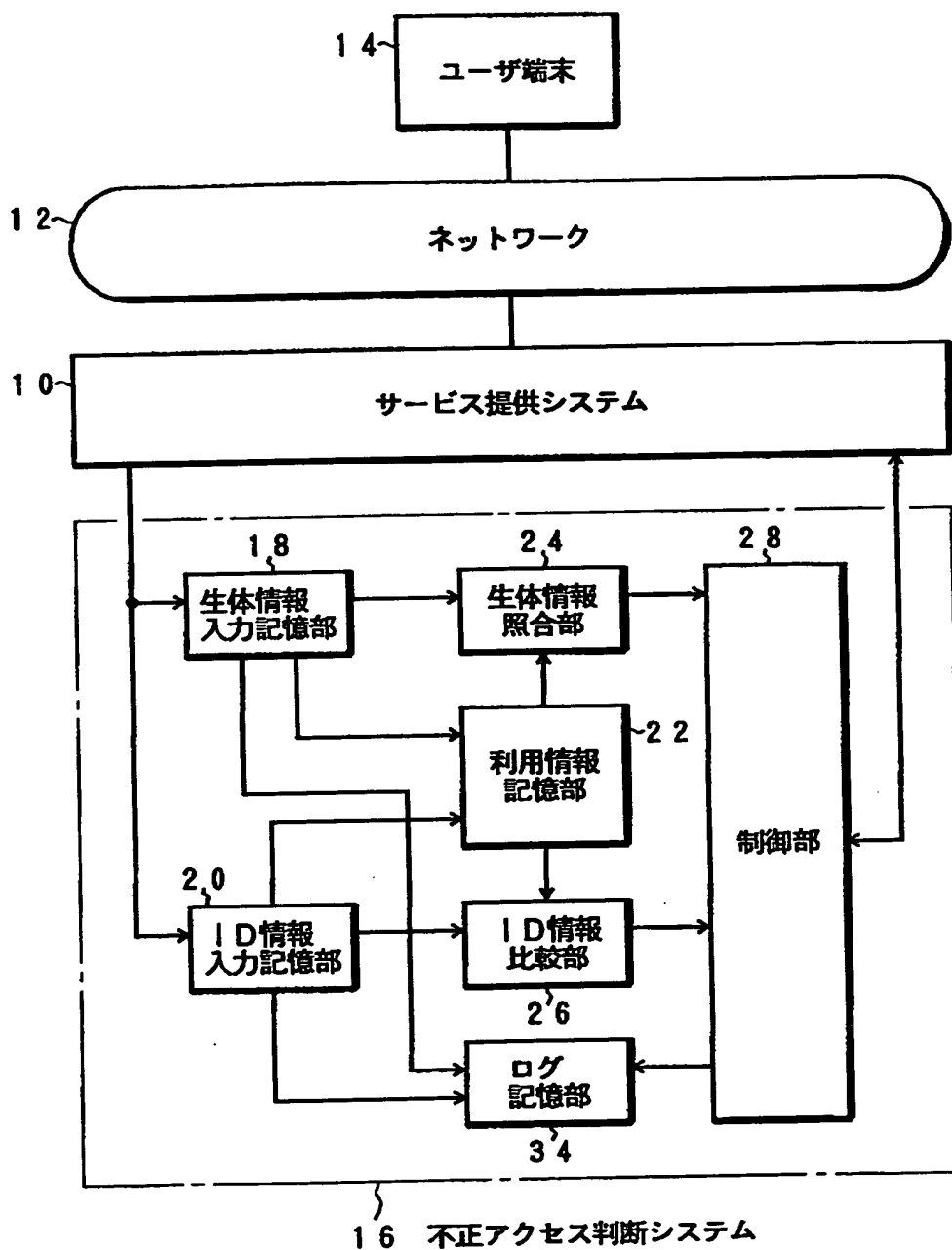
【図 7】

図 2 の不正アクセス判断処理のフローチャート



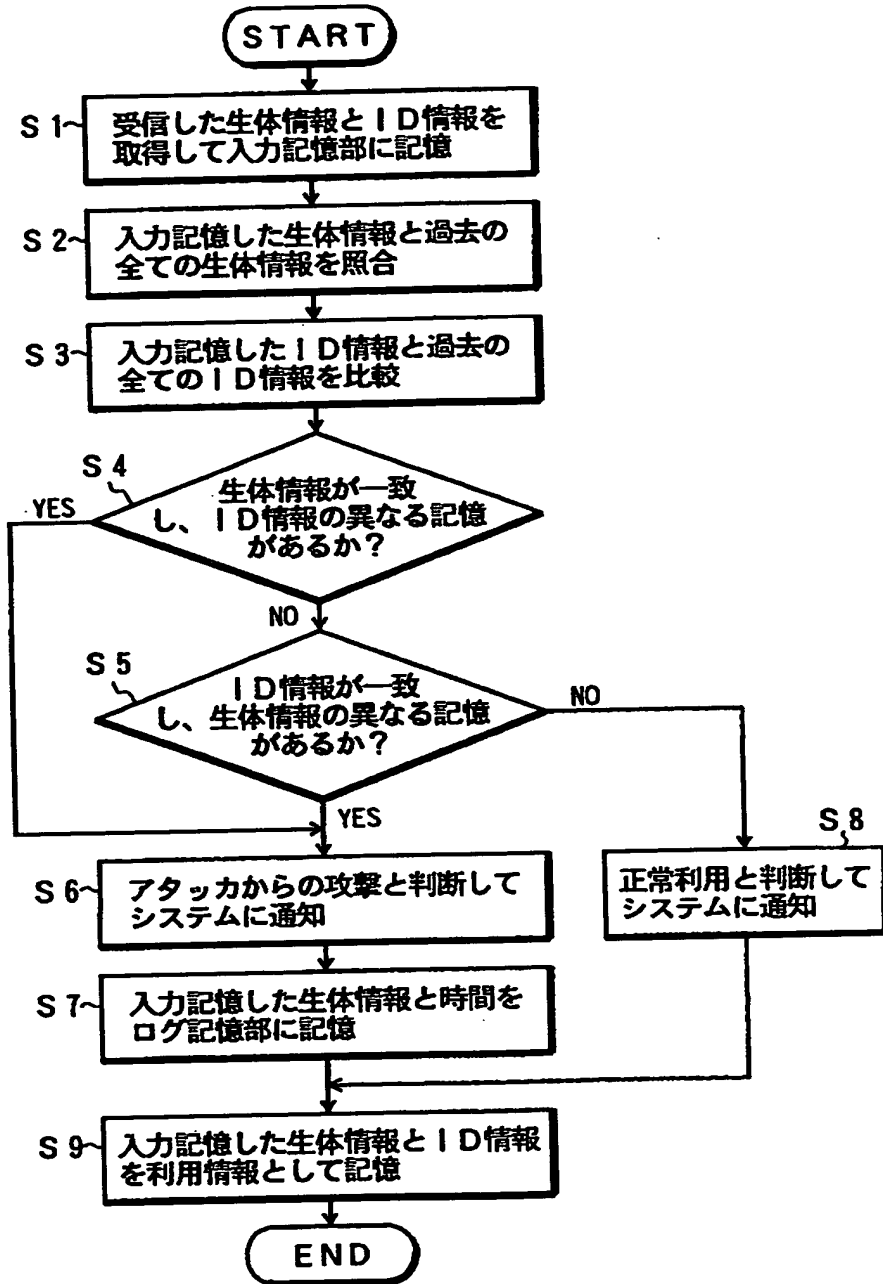
【図 8】

不正アクセス者の身元情報を記憶するログイン機能を備えた本発明の
第2実施形態のブロック図



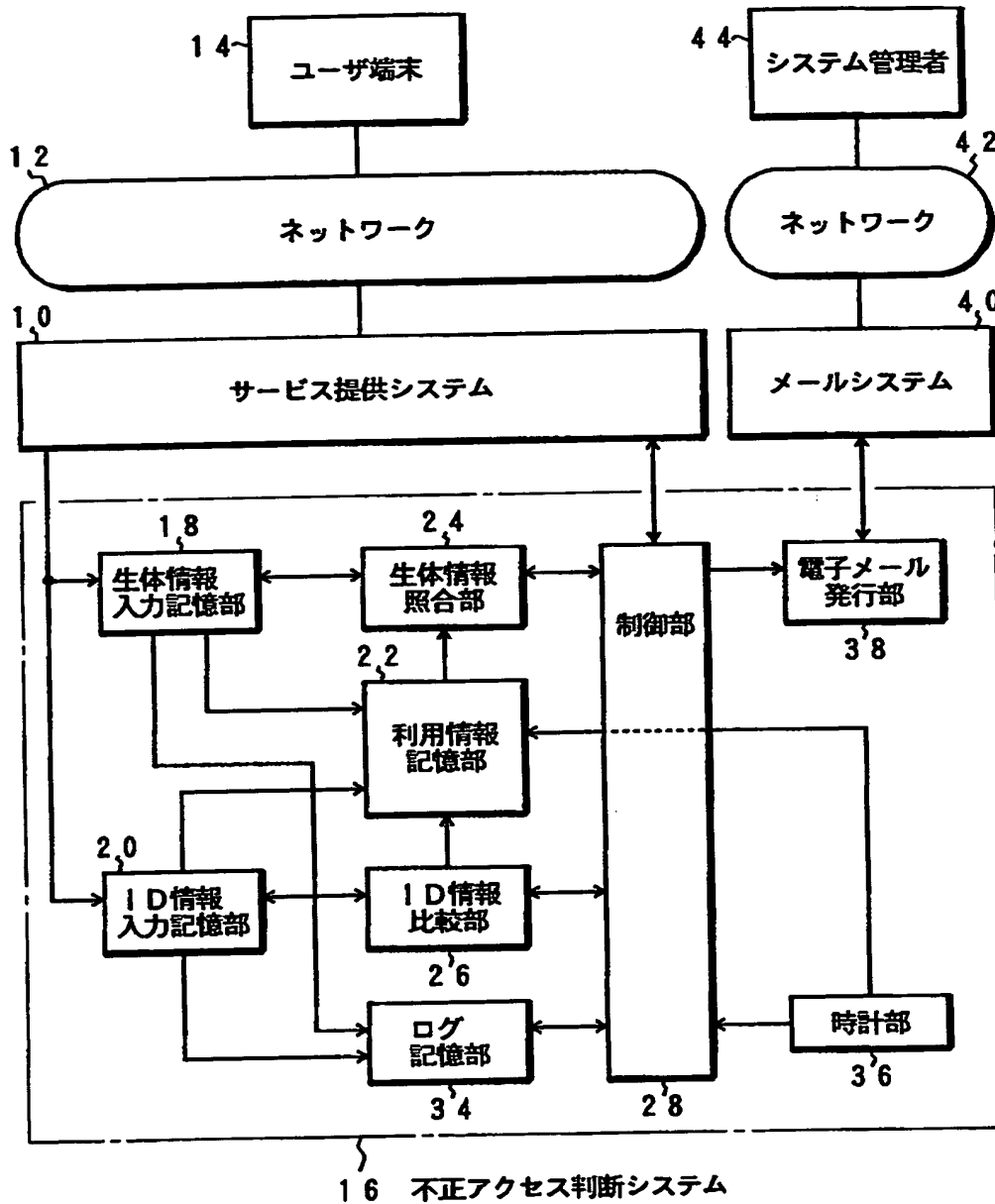
【図9】

図8の不正アクセス判断処理のフローチャート



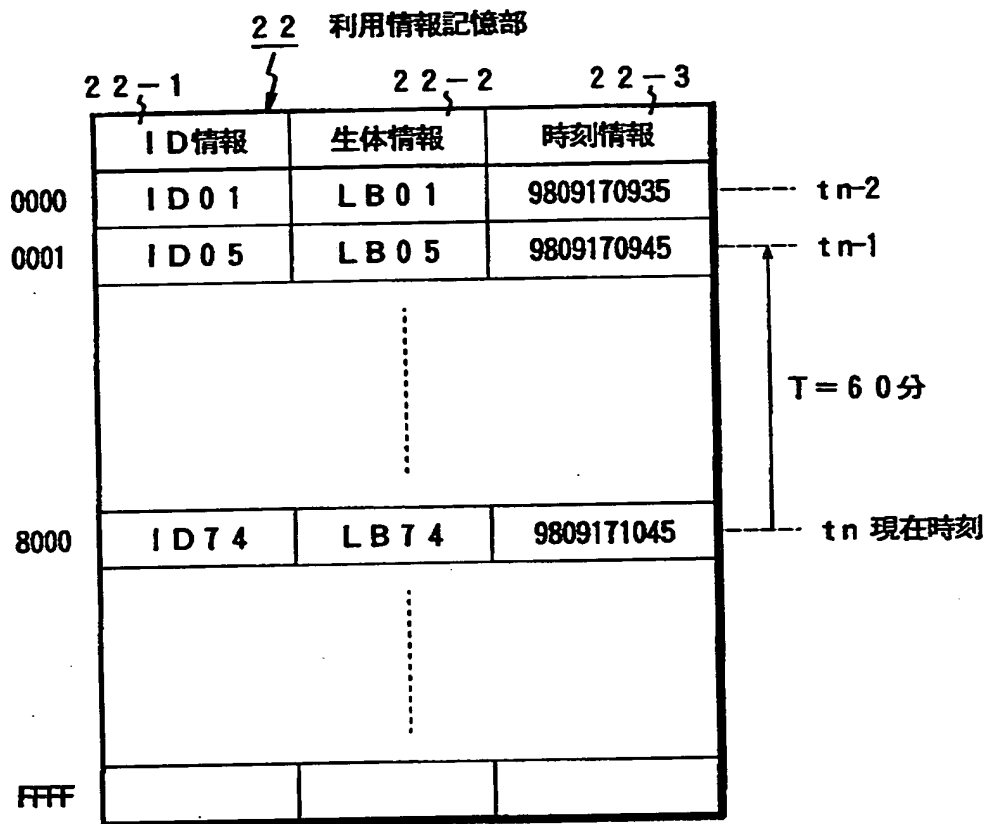
【図 10】

時間計測機能とシステム管理者への自動通報機能を備えた本発明の第3実施形態のブロック図



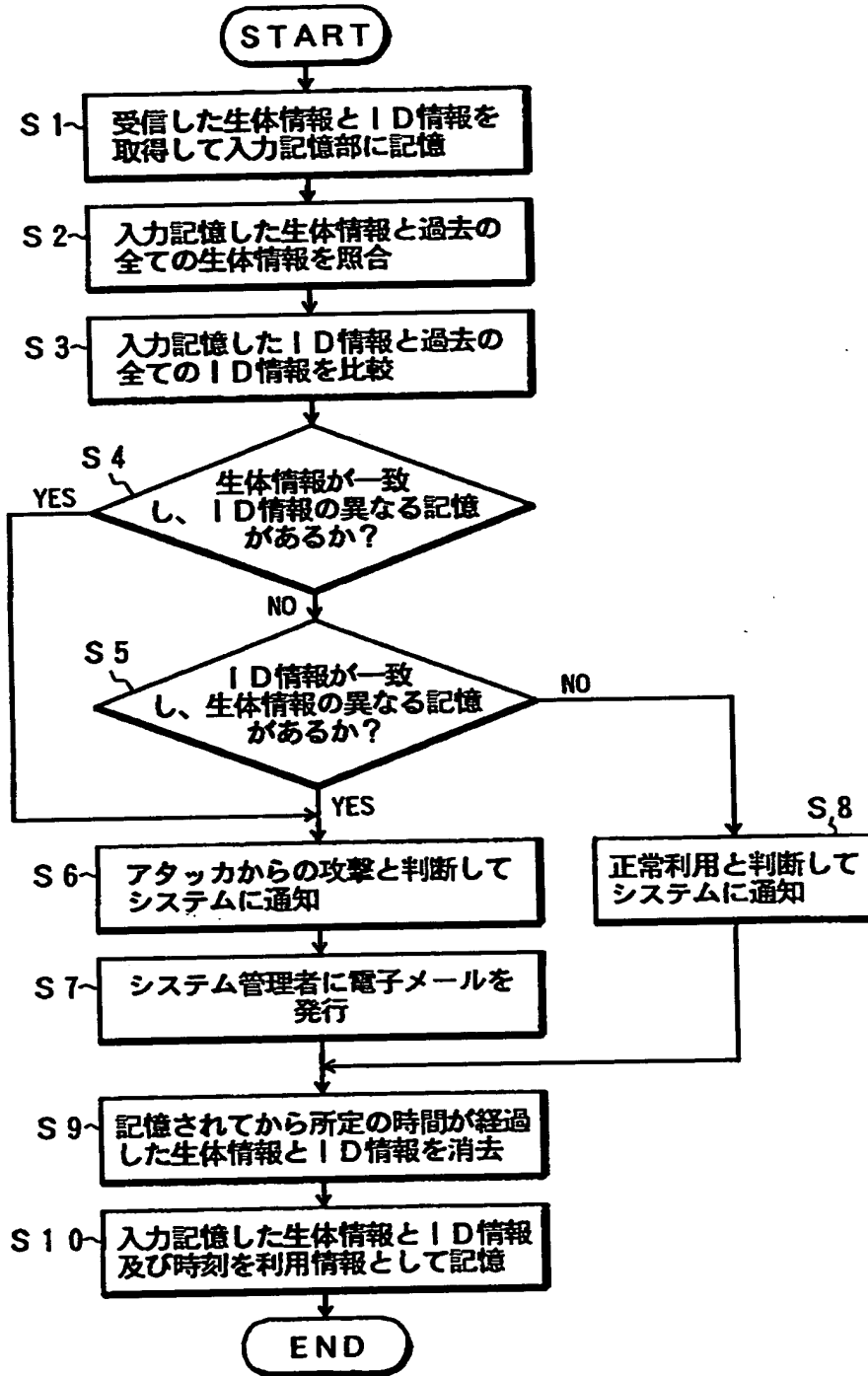
【図 11】

図 10 の利用情報記憶部の説明図



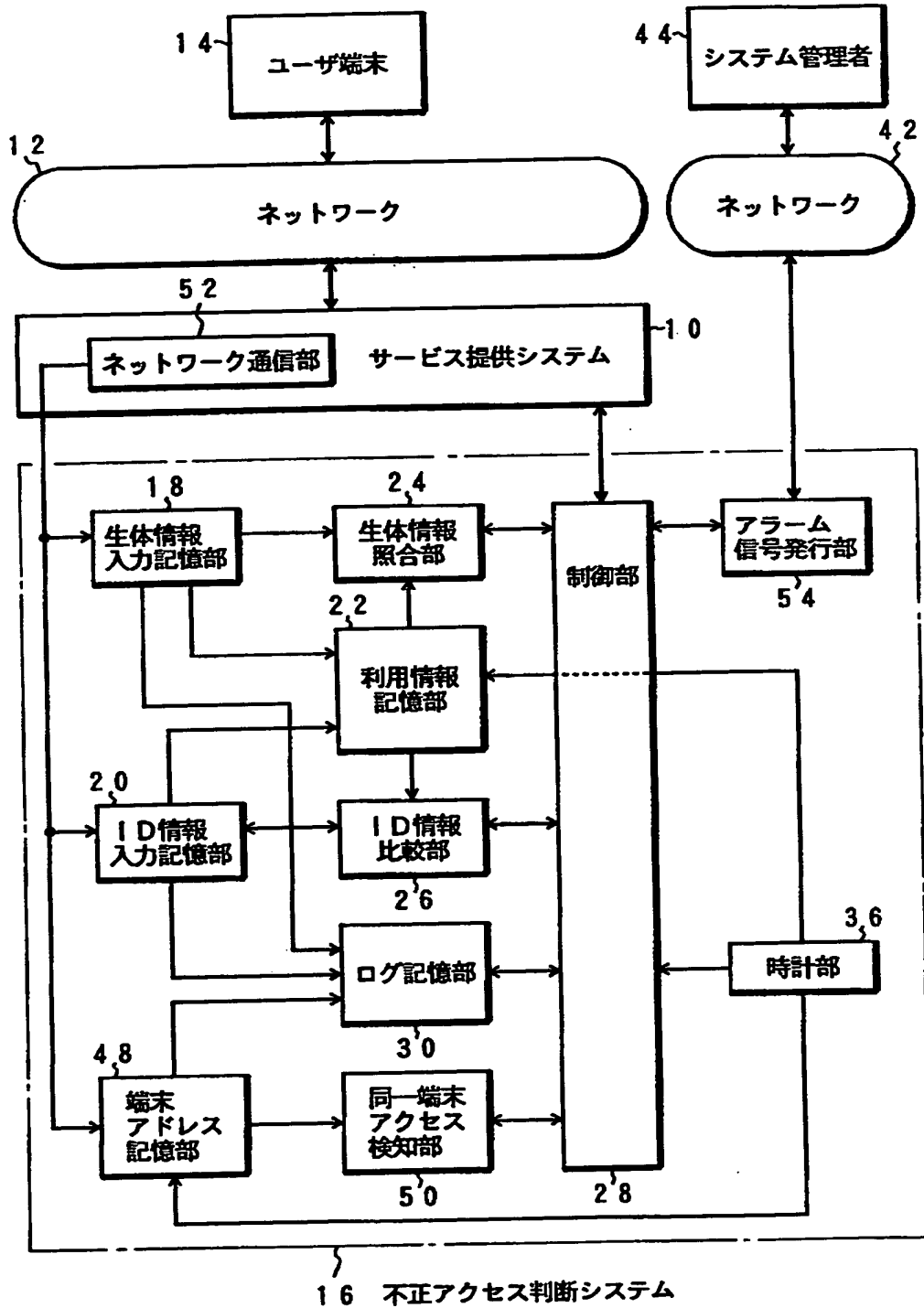
【図 12】

図 10 の不正アクセス判断処理のフローチャート



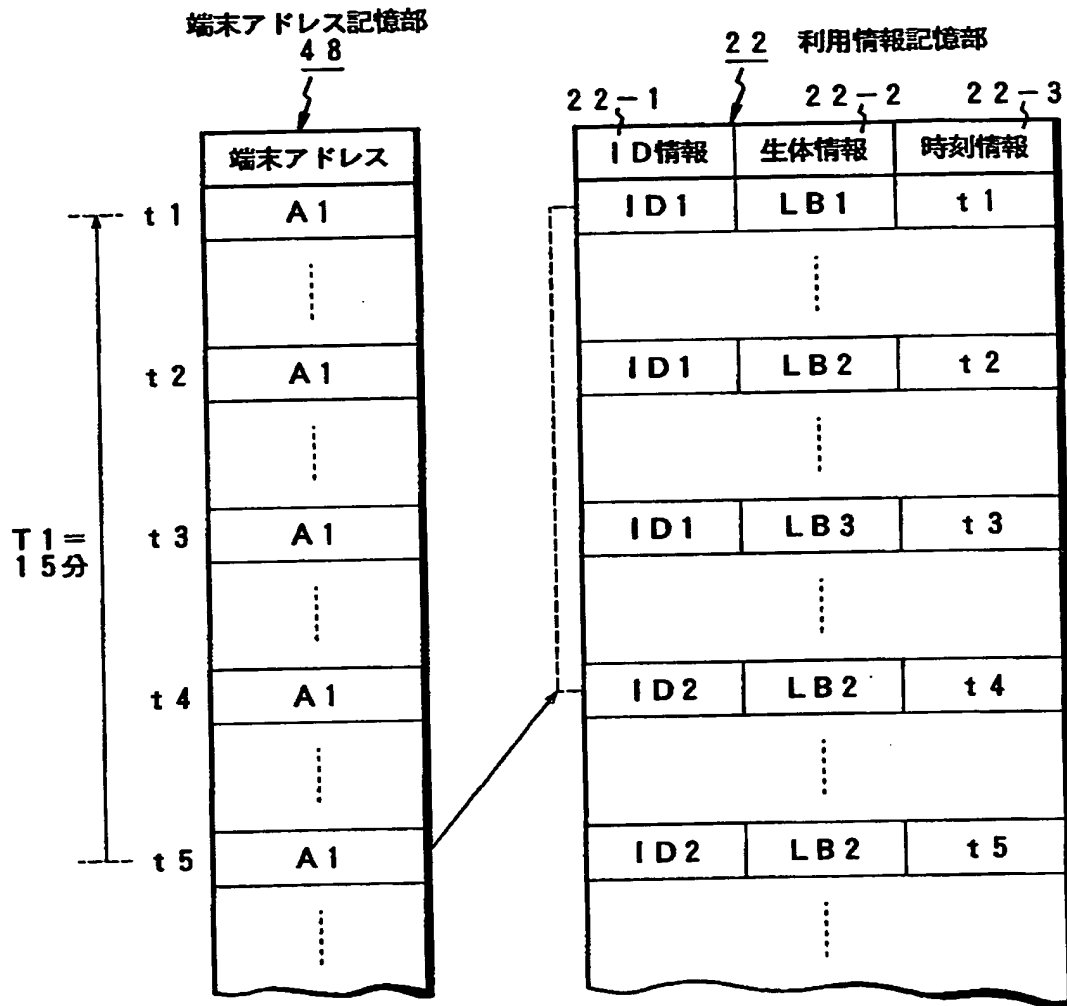
【図 13】

端末アドレスの記憶機能を備えた本発明の第3実施形態のブロック図



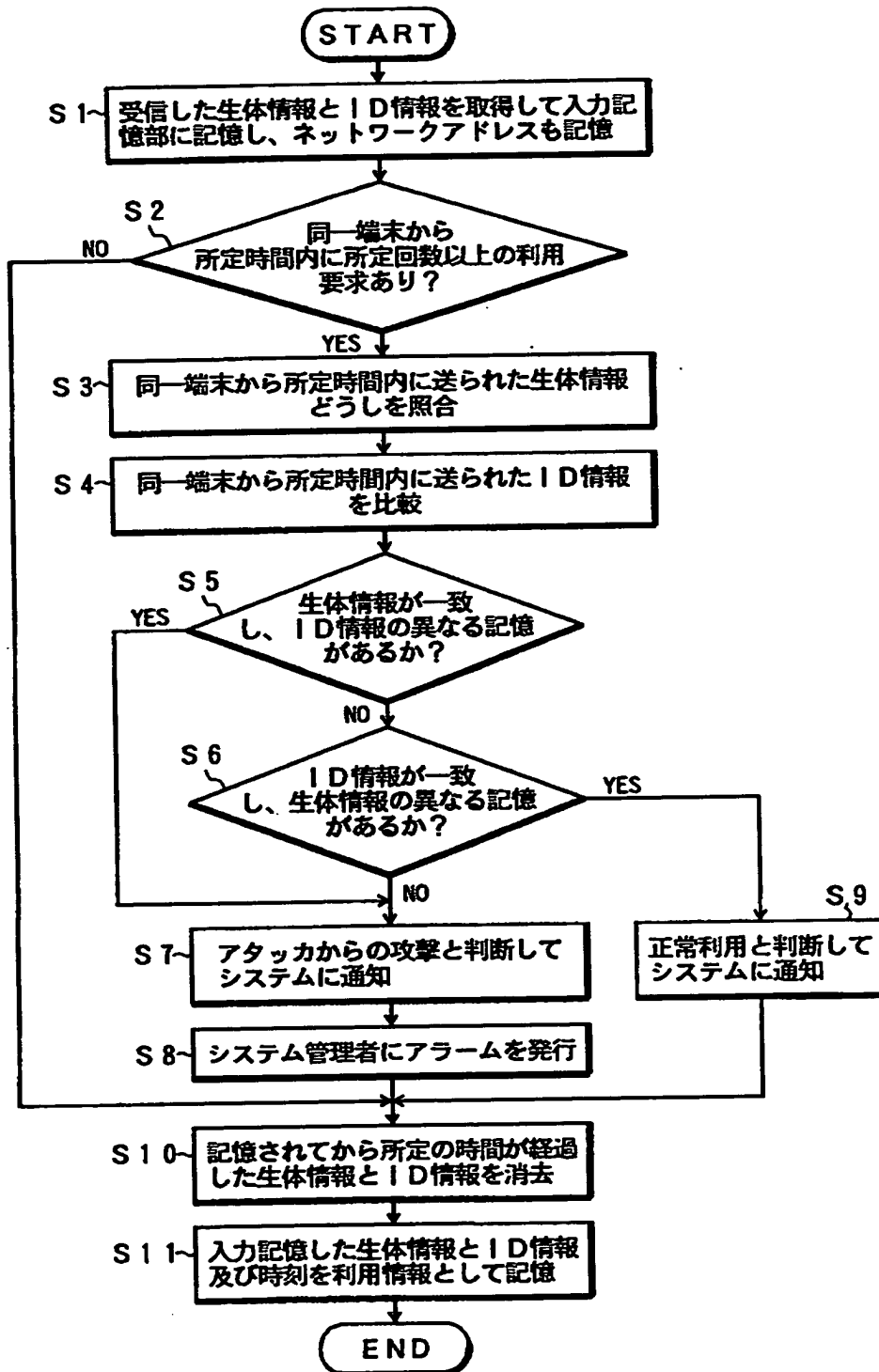
【図 14】

図 13 の端末アドレス記憶部と利用情報記憶部の説明図



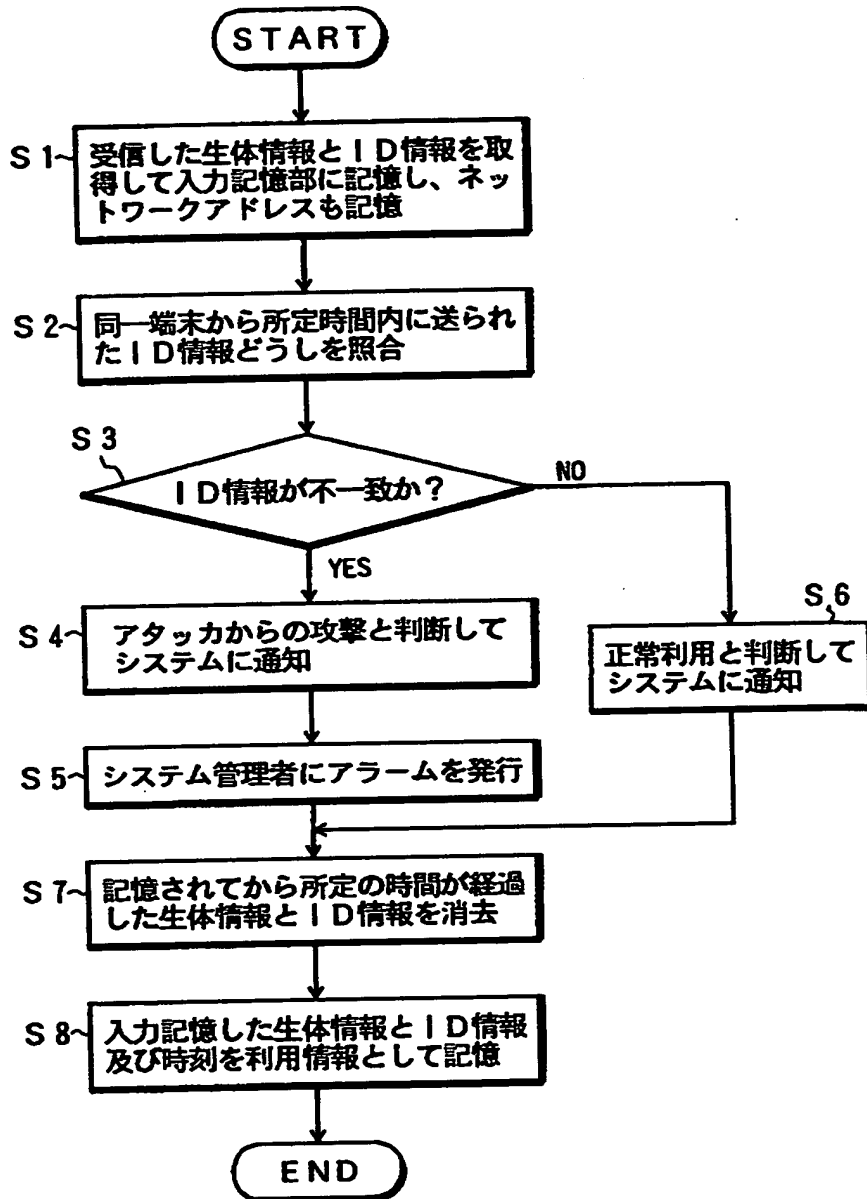
【図 15】

同一端末から所定時間内に所定回数の認証請求があったときに起動する図 14 の不正アクセス判断処理のフローチャート



【図 16】

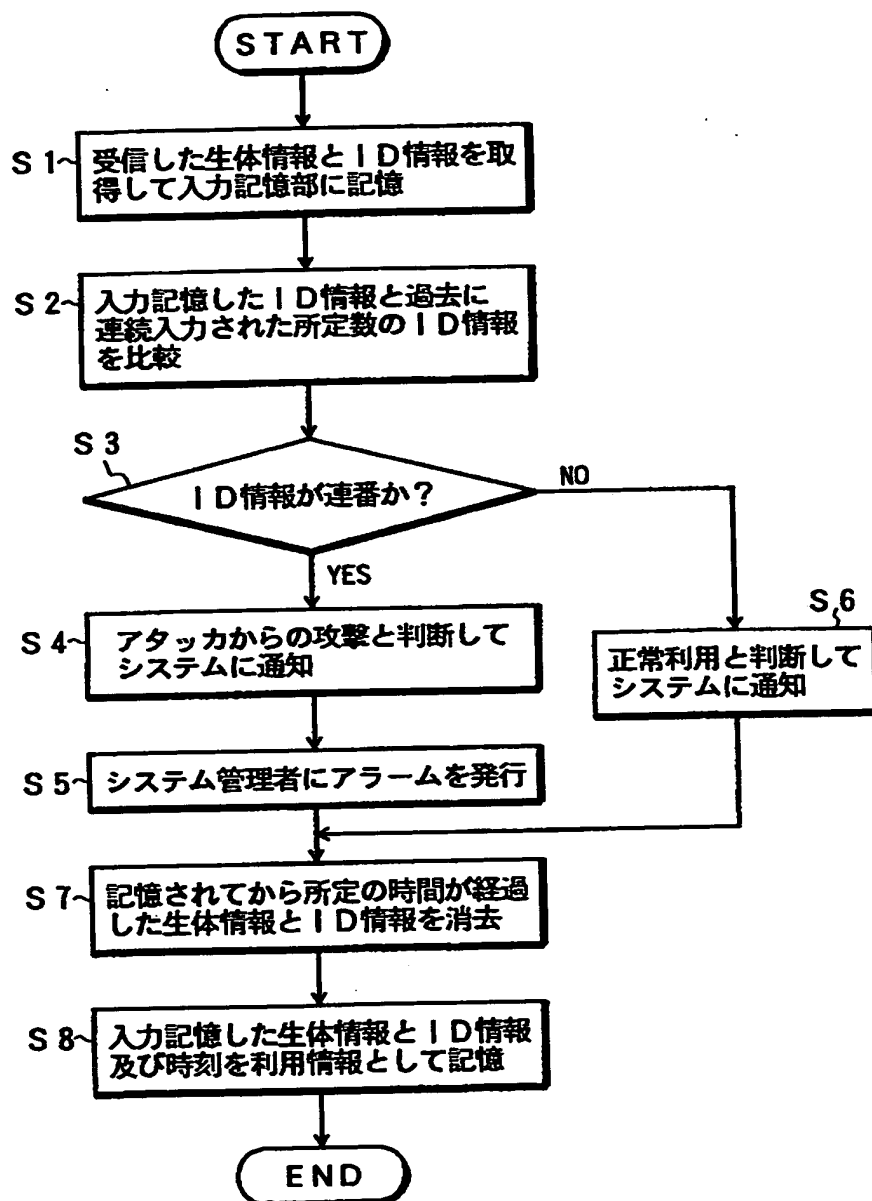
同一端末から所定時間内に入力したID情報のみにより不正アクセスを判断する
判断ルール4が適用される図14の不正アクセス判断処理のフローチャート



【図 17】

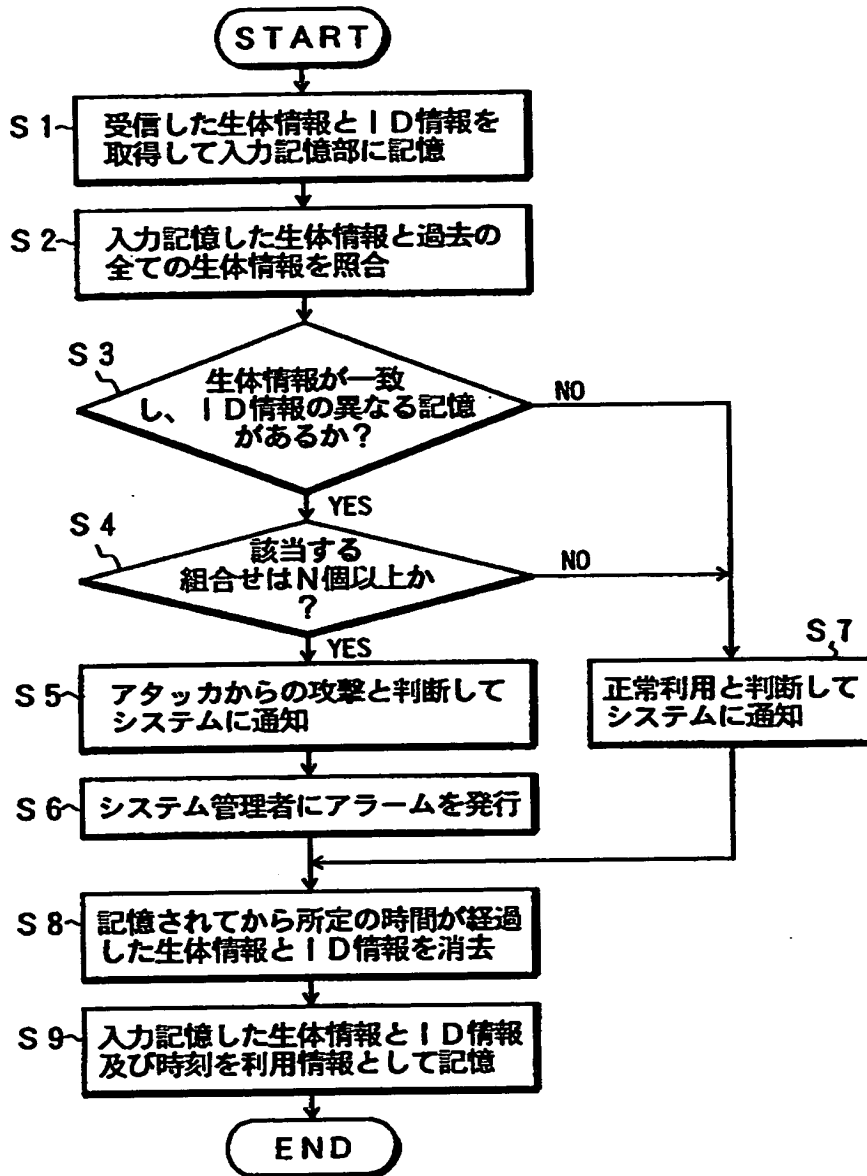
ID情報の連番入力から不正アクセスを判断する判断ルール5が適用される

図14の不正アクセス判断処理のフローチャート



【図 18】

ID情報につき正規ユーザによる誤入力と不正アクセスによる入力を区別する
判断ルール6が適用される図14の不正アクセス判断処理のフローチャート



【書類名】 要約書

【要約】

【課題】 ID 情報と生体情報を使用して本人確認の認証請求行なうサービス提供システムに対する正規ユーザになりすましたアタッカの不正アクセスを監視判断して支援する。

【解決手段】 サービス提供システム 10 が利用者端末 14 から受けた認証請求に基づく ID 情報及び生体情報を入力して利用情報記憶部 22 に記憶し、生体情報入力記憶部 18 と ID 情報入力記憶部 20 の ID 情報及び生体情報と利用情報記憶部 28 に過去に入力された ID 情報及び生体情報とを照合部 24 と比較部 26 で比較照合する。制御部 28 は、比較照合の結果に基づいて不正アクセス者による認証請求を判断してサービス提供システム 10 に通知したり、不正アクセス者の身元情報をロギングする。

【選択図】 図 1

【書類名】
【訂正書類】

職権訂正データ
特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【代理人】 申請人

【識別番号】 100079359

【住所又は居所】 東京都港区西新橋3丁目25番47号 清水ビル8階

【氏名又は名称】 竹内 進

【選任した代理人】

【識別番号】 100093584

【住所又は居所】 東京都港区西新橋3丁目25番47号 清水ビル8階

【氏名又は名称】 宮内 佐一郎

出 願 人 履 歴 情 報

識別番号

[000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社